

**ADMINISTRATIVE SERVICES AGREEMENT**

**BETWEEN**

**VOYA INSTITUTIONAL PLAN SERVICES, LLC**

**AND**

**GOVERNMENT OF THE DISTRICT OF COLUMBIA**

## TABLE OF CONTENTS

	PAGE
1. PLAN PROVISIONS AND SERVICE REQUIREMENTS DOCUMENT .....	3
2. CLIENT RESPONSIBILITIES.....	4
3. SERVICE STANDARDS AND ERROR CORRECTION.....	5
4. COMPENSATION .....	6
5. TERM AND TERMINATION.....	7
6. AMENDMENTS TO THIS AGREEMENT .....	8
7. PLAN AMENDMENTS .....	8
8. CLIENT DIRECTIONS.....	9
9. LIABILITY .....	9
10. INDEMNIFICATION.....	10
11. CONFIDENTIAL INFORMATION AND SECURITY STANDARDS .....	11
12. RIGHTS IN DELIVERABLES AND DATA .....	12
13. COMPLIANCE WITH LAW .....	13
14. SUBCONTRACTING AND ASSIGNMENT .....	14
15. SUSPENSION OF SERVICES .....	14
16. NOTICES.....	14
17. REPRESENTATIONS .....	15
18. RELATIONSHIP OF THE PARTIES .....	15
19. GENERAL PROVISIONS.....	15
EXHIBIT A PLAN PROVISIONS AND SERVICE REQUIREMENTS DOCUMENT	
EXHIBIT B COMPENSATION SCHEDULE	
EXHIBIT C LIST OF PLANS	
EXHIBIT D SERVICE STANDARDS	
EXHIBIT E DATA SECURITY ADDENDUM	
EXHIBIT F RECORDKEEPING EXPENSE ACCOUNT PROCEDURES	
EXHIBIT G POLICY FOR CORRECTION OF INADVERTENT PROCESSING ERRORS	

## ADMINISTRATIVE SERVICES AGREEMENT

THIS AGREEMENT (the "Agreement") is entered into effective as of October 31, 2026, by and between Voya Institutional Plan Services, LLC, a Delaware limited liability company ("Voya"), and the **Government of the District of Columbia** ("Client"), a District of Columbia governmental entity, collectively the "Parties".

### RECITALS

**WHEREAS**, Client has agreed to enter into a relationship with Voya under which Voya will provide certain services to the participants, beneficiaries, alternate payees or other persons with accounts or otherwise entitled to benefits under the Plans (as defined below) ("Participants");

**WHEREAS**, Client desires that Voya, its agents and affiliates perform the plan administration and recordkeeping services ("Services") as specified in the Plan Provisions and Service Requirements Document (the "PPSR"), hereto attached as Exhibit A, with respect to certain benefit plans sponsored by Client, as identified on Exhibit C (each a "Plan" and, collectively, the "Plans");

**WHEREAS**, Voya and Client have reached agreement as to the Services to be rendered to the Plans as set forth in the PPSR; and

**WHEREAS**, the Parties wish to set forth in this Agreement their respective obligations and responsibilities.

**NOW, THEREFORE**, in consideration of the foregoing and the mutual promises contained herein, and subject to the terms and conditions set forth below, Client and Voya hereby agree as follows:

### AGREEMENT

#### 1. SERVICES AND THE PLAN PROVISIONS AND SERVICE REQUIREMENTS DOCUMENT

Client hereby directs Voya to provide the Services as specified in the PPSR. The Services to be rendered and the assumptions underlying the Services to be rendered are set forth in the PPSR. The Compensation Schedule for such Services is attached hereto as Exhibit B of this Agreement. Based upon the assumptions contained therein, Voya agrees to supply the Services on the conditions contained in the PPSR and as provided in this Agreement. The Parties may, from time to time, amend, supplement, or replace the PPSR, or any portion thereof, as provided in Article 6 of this Agreement.

In addition, for more complex financial situations, fee-based financial planning services will also be available to all employees of Client through Voya Financial Advisors, a broker-dealer affiliate of Voya. This service is provided by qualified financial advisors and includes an analysis of the employee's complete financial situation and allows for customized goal planning, including but not limited to retirement income planning, estate planning, social security and pension analysis. Fees for this service will be charged directly to the

employee pursuant to an agreement between the employee and the financial advisor and will not be withheld from an employee's Plan account. This service is offered outside of the Services described in this Agreement and the PPSR.

## 2. CLIENT RESPONSIBILITIES

- 2.1 Provision of Participant Data.** Prior to the commencement of the Services and throughout the term of this Agreement, Client shall furnish or cause to be furnished to Voya all client information ("Client Information") and Participant data ("Participant Data"), as hereinafter defined, necessary for Voya to provide the Services. Participant Data shall mean records and information (whether in hard copy or electronic form) needed to perform services pertaining to Participants and their benefits under the Plans and supplied by Client, any agent of Client, including but not limited to, any prior recordkeeper, trustee, custodian, broker/dealer, insurance company, mutual fund company, third party administrator and any other entity that provided services to the Plan, Participants or created by Voya or its subcontractors in the course of providing the Services. Client Information shall mean any and all data or information (in whatever form or media) that is owned or developed by or licensed to Client and that is supplied to Voya by Client. All such Client Information and Participant Data shall be provided in a timely manner and in formats agreed upon by Client and Voya and shall be complete in all material respects. Voya's obligation to provide the Services in accordance with the PPSR and other deadlines under this Agreement is contingent upon the timely receipt of all relevant Client Information and Participant Data from Client that is complete and conforms to the formats and specifications agreed to in advance by Client and Voya. Client shall be solely responsible for the accuracy and completeness of any such Client Information and Participant Data and shall promptly furnish or cause to be furnished accurate and complete Client Information and Participant Data to correct any inaccuracies or incompleteness with respect to Client Information and Participant Data previously provided to Voya. Client shall promptly notify Voya in writing of any claimed error with respect to any Participant Data or report as soon as practicable. In no event will Voya be liable for correction of any such identified error to the extent that it resulted from erroneous Client Information or Participant Data.
- 2.2. Selection of Investment Options.** Client shall be responsible for the selection of all investment options under the Plans. Voya shall have no responsibility or discretion under the terms of this Agreement for the prudence, selection or oversight of any investment options under the Plans. Client acknowledges and agrees that (i) all investment information or investment materials that may be provided by Voya to Client are provided to enable Client to independently assess available options and make investment decisions for the Plans and (ii) Voya's 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 Client may consider making available under the Plans.
- 2.3 Plan Qualification.** Client represents that each Plan identified in Exhibit C of this Agreement meets the

requirements of Section 401(a) of the Internal Revenue Code, as amended (the “Code”), Section 457(b) of the Code, and other provisions of the Code applicable to such Plan.

Client agrees to use its best efforts to operate each Plan in accordance with applicable law including the requirements of the Code and consistent with the representation given in this Section 2.3. Upon the occurrence of any event that would have a material adverse effect on any Plan’s compliance with the requirements of the Code or that would cause the applicable representation given above to be untrue, Client will immediately notify Voya in writing specifying the nature of such occurrence. Client shall take all measures required under current federal law and applicable provisions of the Code and related regulations to assure the qualification of each Plan that is intended to be a qualified plan, including without limitation the timely preparation of each Plan amendment required by the Code and related regulations. Voya shall be under no duty to question the measures taken by Client pursuant to this Section 2.3.

- 2.4 Plan Interpretation.** Client shall provide legal and other technical assistance as necessary or appropriate to furnish Voya with the proper interpretation and operation of the Plans and shall verify that any Client Direction (as defined below) is consistent with the terms of the Plan. Voya shall not be responsible for the interpretation of the Plans

### **3. SERVICE STANDARDS AND ERROR CORRECTION**

- 3.1 Service Standards.** Voya represents that (i) its Services shall conform in all material respects with the PPSR; (ii) it will use due care in providing the Services and (iii) it will use its best efforts to maintain the equipment, computer software, interactive voice response systems, other technological systems and related documentation used by Voya to provide the Services (the “Voya System”), so that the Services are furnished in a manner which complies with all applicable federal laws and regulations as are in effect from time to time. The Services shall conform to prevailing industry standards for comparable services. In addition, Voya and Client have identified certain minimum performance standards as detailed in Exhibit D (“Service Standards”). Service Standards shall be applicable only to the extent all material information necessary for the successful delivery of Services subject to the Service Standards is received by Voya in “Good Order” (as such term is defined in Exhibit D). Voya’s payment of any Service Standard penalties and/or waiver of any fee amounts otherwise payable to Voya shall not constitute an admission of liability or violation of applicable law and shall reflect, solely, a contractual obligation as provided in this Agreement and Exhibit D.

- 3.2 Error Correction.**

(a) **Voya Error.** Voya shall promptly notify Client after becoming aware of an error resulting from the acts or omissions of Voya 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, Client's determination or approval of the correction to be applied to such error.

(b) **Client Error.** Client shall promptly notify Voya after becoming aware of an error resulting from the acts or omissions of Client, its agents or third parties, or otherwise caused by the negligent acts of Client, its agents or third parties. Voya will attempt to correct such errors at Client's expense and subject to Voya's receipt of all data reasonably necessary to make such correction. Client shall pay Voya its reasonable expenses incurred in making such corrections.

#### 4. COMPENSATION

4.1 **General.** As consideration for Voya's performance of the Services, Client agrees to pay Voya the fees set forth in Exhibit B of this Agreement.

4.2 **Additional Services.** If Voya provides services in addition to the Services set forth in the PPSR, Voya shall be entitled to be compensated for such additional Services in such amount as the Parties mutually agree in a written amendment to Exhibit B of this Agreement. Proposals for changes to the Services will be governed by the provisions of Article 6.

4.3 **Invoicing and Payment.** Voya shall provide Client with an invoice for any Services performed. Client represents and warrants that the Plans provide that fees for services rendered to the Plans shall be paid by the Plans from Plan assets unless voluntarily paid for by the Plan sponsor on behalf of the Plans. Voya shall automatically charge all fees against the Plans unless otherwise directed by Client. A late payment charge of 1.5% per month will be assessed on overdue accounts. In the event that Client disputes any invoice, or portion of any invoice, it shall pay any undisputed portion of the invoice and escrow the disputed portion until resolution of the dispute.

4.4 **Effective Date of Fees.** The fees specified in Exhibit B shall remain in effect as provided in Exhibit B to this Agreement.

4.5 **Other Compensation.** Voya has entered into contracts with certain investment funds and fund service providers (the "Funds") pursuant to which such Funds compensate Voya for administrative and sub-transfer agency functions performed by Voya or its affiliates and calculated with reference to the aggregate assets of Voya clients' plans under management by such Funds and/or on a per-participant basis investing in the Funds. Any amounts payable by the Funds ("Fund Revenue") shall be paid directly to Voya. As provided in Exhibit F, Voya shall deposit an amount equal to the Fund Revenue relating to a Plan into the recordkeeping expense account established for the Plan within the Plan's trust ("Recordkeeping Expense Account"). Amounts held within the Recordkeeping Expense Account shall be available to pay qualified ERISA expenses in connection with the administration of the Plan as determined by Client and/or be allocated to

Participant accounts upon written direction from Client. It shall be the sole responsibility of Client to determine whether expenses are qualified ERISA expenses and are properly payable from the Recordkeeping Expense Account. Client hereby represents that either Client, or another fiduciary independent of Voya, has (i) made the decision on behalf of the Plans to invest in the investment options selected for the Plans or to offer the Funds as investment options under the Plans, as the case may be, and (ii) been fully informed of, and approved of, Voya's fee arrangement, if any, with respect to each such Fund prior to making such investment decision.

Client acknowledges that if Voya establishes one or more bank accounts ("Accounts"), either directly or through a custodian or other subcontractor, to hold (i) Plan contributions pending investment direction and/or (ii) amounts pending distribution from the Plan, any earnings credited to Voya based on amounts held in the Accounts ("Float") shall constitute a part of overall compensation of Voya. To the extent that Float is earned on Plan contributions pending investment direction, such amounts shall be invested in accordance with procedures as described in the PPSR, or as otherwise directed by Client. To the extent that Float is earned on Plan distributions, the period during which the Float will be earned commences on the date the check is written and ends on the date the check is presented for payment, if not stale-dated at the time of presentation. Stale-dated check amounts will be returned to the Plan trust as provided in the PPSR. Distribution checks are mailed U.S. first class mail, unless otherwise directed by the Participant or Client, within the timeframe prescribed by the PPSR.

Voya, acting on behalf of its affiliated directed trustee, shall earn interest on check Float at a rate to be set each month. Voya shall retain a portion of these earnings equaling 1.25% annually to offset related costs including third party services, such as check writing and related banking and tax services, services supporting payments, and postage for check, tax forms and other related materials. Voya shall rebate the remaining earnings to the Plan. The amount rebated to Client shall be credited to Client on a monthly basis based on the average outstanding check balance over the month.

- 4.6 Transaction Processing Errors.** Voya processes investment instructions on an "omnibus" or aggregated basis. If Voya's correction of a Voya processing error results in a loss to a Plan 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. For more information on Voya's error correction policy, please refer to the attached Policy for Correction of Processing Errors ("Policy"). The Policy and any updates to the Policy will be posted in the Sponsor Disclosure section of the plan sponsor website.

## **5. TERM AND TERMINATION**

- 5.1 Initial Term; Continuation.** Upon execution by both Parties, this Agreement shall commence on the effective date stated above (the "Effective Date") and shall remain in effect for a period of five (5) years after Voya commences providing ongoing Services. After five (5) years, Client may extend the term of this Agreement for a period of two (2) year two (2) option periods, or successive fractions thereof, by written notice to Voya before expiration of the Agreement, provided that Client will give Voya preliminary written notice of its intent to extend before the contract expires.

The preliminary notice does not commit Client to an extension, the exercise of this option is subject to the availability of funds at the time of the exercise of this option. This section is subject to the termination provisions of Section 5.2 of this Agreement. In the event that this Agreement is terminated without cause by Client pursuant to Section 5.2(a) prior to the expiration of the initial five (5) year term, Client shall, to the extent permitted by law, reimburse Voya for any unrealized implementation and initial Participant communication expenses as set forth in Exhibit B to this Agreement.

## **5.2 Termination.**

(a) **Without Cause.** Either Party may terminate this Agreement at any time without cause by giving at least one hundred eighty (180) days prior written notice of such termination to the other Party.

(b) **With Cause.** Either Party may terminate this Agreement at any time (i) for cause upon the breach of any material obligation or responsibility by the other Party which breach remains uncured for sixty (60) days after written notice thereof has been provided to the breaching Party by the other Party, or (ii) immediately and without the necessity for notice, upon the bankruptcy, insolvency or similar filing or event by or against the other Party.

**5.3 Cooperation with Transfer.** In the event of any termination of this Agreement, Voya shall cooperate with Client in the transfer of Voya's obligations hereunder to a replacement service provider ("Transition Assistance").

## **6. CHANGES TO THE SERVICES AND AMENDMENTS TO THIS AGREEMENT**

The Parties may amend any aspect of this Agreement pursuant to a written amendment to this Agreement executed by the Parties. Any amendment shall not be effective until fully executed by the Parties.

Either Party may from time to time propose a change to the Services, and the Parties agree to meet promptly to discuss such proposed change. Any change to the Services agreed to by the Parties shall be documented in a change order that includes a description of the change and any implementation costs. If a change to the Services results in a change to the fees contained in Exhibit B hereto, the parties agree to promptly negotiate and execute an amendment to Exhibit B to reflect such change(s) to the fees. Costs incurred by Voya in connection with Voya's implementation of additional Services, or implementation of changes to existing Services, will be the responsibility of Client unless the Parties agree otherwise.

To the extent a service enhancement is provided by Voya or a change to the Services is required by a change in applicable legal or regulatory requirements, no express consent by Client to a change order or amendment to this Agreement shall be required.

## **7. PLAN AMENDMENTS**

Voya shall be under no obligation to provide Services in accordance with any Plan's amendments proposed by Client until Voya has been given at least ninety (90) days to review such amendments to identify and assess potential impacts to the Voya System and Client and Voya have agreed to an implementation plan for any resulting changes to the Voya System. If a Plan amendment affects the Services, Voya and Client shall comply with the procedures set forth in Article 6. Voya's acting in accordance with Plan amendments shall constitute Voya's acquiescence to the use of the documents involved and not its



approval of their contents or their effect. Client shall assume full responsibility to Voya and to all interested persons for such contents and such effect. Further, Voya shall be under no duty to question measures taken by Client with respect to such Plan amendments.

Voya shall provide necessary changes to the Plans as needed resulting from state and/or Federal legislation without additional costs to Participants under the terms of this Agreement.

## 8. CLIENT DIRECTIONS

- 8.1 General.** In the course of providing the Services, Voya may receive written or oral instructions or directions from representatives of Client, including its legal counsel (hereinafter collectively referred to as "Client Directions"), concerning the provision of Services. Client 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 Plans; (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. Upon receipt of Client Directions, Voya shall promptly indicate acceptance of Client Directions or notify Client in writing that it will not be able to comply with such Client Directions and provide a description of the reasons therefor. Voya may, but shall not be required to, inquire into the genuineness of any Client Direction or require written confirmation thereof. The PPSR shall be deemed to be a standing Client Direction.
- 8.2 Reliance.** Voya may rely upon and comply with any Client Direction in performing its obligations under this Agreement. If and to the extent that Voya or any of its subcontractors act or fail to act as a result of reasonable reliance upon any Client Direction or any information, data, document or instrument supplied by Client 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 Client and does not receive a Client 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.
- 8.3 Conflict with Agreement.** If any Client Direction is inconsistent with or conflicts with any provision of this Agreement or the PPSR, Voya may, at its discretion, require that such Client Direction be confirmed in writing by an authorized representative of Client.

## 9. LIABILITY

- 9.1 Insurance.** Voya shall at all times during the term of this Agreement, at its own cost and expense, carry and maintain commercially reasonable insurance coverage.
- 9.2 Disclaimer of Certain Damages.** NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, REGARDLESS OF THE FORM OF ACTION, WHICH MAY

ARISE FROM THE PERFORMANCE, NONPERFORMANCE, BREACH OF WARRANTY, DEFAULT OR OTHER BREACH OF THIS AGREEMENT.

- 9.3 Damages.** Subject to Section 9.2, Voya's aggregate liability for any and all claims, whether based on performance, nonperformance, breach of contract or warranty, events of default, tort, strict liability or otherwise, shall be limited to direct damages attributable hereunder to the conduct of Voya. If Client properly terminates this Agreement due to Voya's material breach as provided in Section 5.2(b), Client's direct damages under this Article may include the out-of-pocket costs incurred in securing a replacement contractor, or transferring the functions back to Client, but such damages shall not include any ongoing costs of providing such replacement Services. Neither Party shall be liable to the other for damages of any type (other than late payment charges) with respect to any nonperformance, breach or default which is cured during the applicable cure period described in Section 5.2(b).
- 9.4 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 Client Directions or information, data documents or instruments provided by Client 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.

## 10. INDEMNIFICATION

- 10.1 Voya's Indemnity of Client.** Voya shall be responsible to Client for any and all Losses, and shall defend, indemnify, and hold Client harmless from and against any and all Participant or third-party actions, suits, proceedings, claims or liability, arising from Voya's negligence, willful misconduct or bad faith in the performance or nonperformance of this Agreement or Voya's violation of applicable law. Client shall have an obligation to take all reasonable steps to mitigate any Losses. In the event that Client refuses or fails to take action to do so and such refusal or failure is unreasonable, Voya shall be relieved of its responsibility to indemnify Client hereunder.
- 10.2 Apportionment of Liability.** With respect to any matter that is described in Section 10.1, liability shall be apportioned between Client and Voya in proportion to the extent to which each is responsible for causing the matter to arise.
- 10.3 Liability for Plan Obligations.** Client or the Plans shall remain solely liable for all obligations and benefits payable under the terms of the Plans and applicable law.
- 10.4 Participation in Defense.** A Party may participate at its expense in the defense of any action or claim which may be asserted against it and for which such Party seeks indemnity pursuant to the provisions of this Article, or such indemnified Party may assume the defense of such claim or action, including the right to settle or compromise any claim against it without the consent of the indemnifying Party,

provided that in doing so it shall be deemed to have waived its right to indemnification except in cases where the indemnifying Party has declined to defend the claim. Otherwise, the indemnifying Party shall have exclusive authority to control the defense, conduct settlement negotiations and may settle an action, suit, proceeding or any matter for which indemnification is sought, without the indemnified Party's consent; provided, however that such settlement includes a release of the indemnified Party with respect to the matter for which indemnification is sought.

**10.5 Indemnified Persons.** In this Article, references to Client and Voya shall be deemed to include their respective partners, members, directors, officers, agents, employees, attorneys, affiliates and subcontractors.

**10.6 Errors of Other Service Providers.** Voya shall bear no obligation or responsibility for Losses 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.

## 11. CONFIDENTIAL INFORMATION AND SECURITY STANDARDS

**11.1 Confidential Information.** The Parties agree that the provisions of the Data Security Addendum, attached hereto as Exhibit E, shall govern the treatment of Confidential Information (as such term is defined in Exhibit E) received by a Party under this Agreement.

**11.2 Security Standards.** Client agrees that it shall comply with Voya's minimum information security standards ("Security Standards") as needed to enable Voya to perform the Services. The Security Standards include, but are not limited to, controls and practices designed to safeguard Participant accounts from potentially fraudulent activity. The current Security Standards have been received by Client prior to the Effective Date and will thereafter be provided to Client upon reasonable request. Voya may revise the Security Standards as it deems appropriate and shall use its best efforts to provide Client with a copy of any such revision at least ninety (90) days prior to implementation of the resulting changes on the Voya System. Notwithstanding any other provision of this Agreement, Client's failure to comply with the Security Standards shall relieve Voya of all liability for any Losses (as defined in Section 10.1) arising from such failure.

## 12. RIGHTS IN DELIVERABLES AND DATA

**12.1 Deliverables.** Client shall have the right, subject to the limitations set forth in this Agreement, to reproduce, use and dispose of all or any part of the reports, or records, documents, data and other materials to be delivered to Client pursuant to this Agreement in administering the Plans.

**12.2 Intellectual Property.** Nothing contained in this Agreement shall confer to Client any property rights, proprietary interest, copyright or license in the assets or technology of Voya, including, without limitation, the software, upgrades and enhancements to the software, written materials, screen formats and designs, techniques, interactive design techniques, report formats, interactive design formats, systems or know-how used or developed to provide the Services. Client acknowledges that such assets and technology constitute copyrighted trade secrets or proprietary information of substantial value to Voya. Nothing in this Section 12.2 alters or impacts the Client's ownership and rights in data as provided

by Section 12.3, below. Client agrees that it shall treat the foregoing assets and technology as proprietary to Voya and that it shall not divulge any of such proprietary information to any person or organization except as expressly permitted herein. Without limiting the foregoing, Client agrees for itself and its employees and agents:

- (a) to use such programs and data bases solely in accordance with Voya's applicable user documentation;
- (b) to refrain from copying or duplicating in any way any part of the Voya System;
- (c) to refrain from obtaining unauthorized access to any programs, data or other information not owned by Client, and if such access is accidentally obtained, to respect and safeguard the same as Confidential Information of Voya;
- (d) that Client shall have read-only access to only those authorized transactions as agreed to between Client and Voya;
- (e) to honor reasonable written requests made by Voya to protect at Voya's expense the rights of Voya in the Voya System and other proprietary information at common law, under the federal copyright statutes and under other federal and state statutes; and
- (f) to use the equipment, computer programs and other information supplied by Voya under this Agreement solely for its own internal use and benefit in administering the Plans and not for resale or other transfer or disposition to, or use by or for the benefit of, any other person or organization without prior written approval of Voya.

**12.3 Participant Data and Client Material.** All of the Participant Data, Client Information and any other materials pertaining to Client's requirements or the Plans and provided to Voya by Client pursuant to this Agreement shall at all times remain the property of Client. Notwithstanding the foregoing, Voya shall use Participant Data to the extent and for purposes authorized by the Participant whose data is being used.

**12.4 Inspection.** During the term of this Agreement and for thirty-six (36) months following the termination of this Agreement, Client, may upon written notice, request copies of data and materials used to provide the Services. Voya may require the execution of additional confidentiality agreements in connection with any such request for data and Plan information.

**12.5 Production of Documents.** The charges under this Agreement do not include Voya's fees and expenses for any costs, including legal costs, associated with considering or responding to requests for documents, providing testimony, or participating in legal or regulatory proceedings as a result of the performance of the Services. Voya shall invoice Client separately for such reasonable fees and expenses.

### **13. COMPLIANCE WITH LAW**

**13.1 Filing of Tax Returns and Form 5500.** Although Voya may provide data used in such returns, forms or information, Voya shall not be responsible for the filing of any federal, state or local tax return, forms or information on behalf of Client or any Plan unless specifically described in the PPSR.

- 13.2     Required Disclosure.** Voya has disclosed in writing, to the best of Voya's knowledge, the information required to be provided to Client by 29 CFR § 2550.408b-2(c) (the "DOL Regulation"). Voya hereby represents that, prior to the date hereof, all such information was provided to Client.
- 13.3     Disclosure of Changes.** Voya shall disclose to Client any change to the information required to be provided to Client by the DOL Regulation, such disclosure to be effected not later than thirty (30) days from the date Voya acquires knowledge thereof.
- 13.4     Additional Information.** Voya shall disclose to Client all information related to this Agreement and the Services, including any compensation or fees received thereunder, that is requested by Client or by the administrator of any Plans in order to comply with the reporting and disclosure requirements of Title I of ERISA and the regulations, forms and schedules issued thereunder.

## 14. SUBCONTRACTING AND ASSIGNMENT

- 14.1 Subcontracting.** Voya may enter into one or more subcontracts in connection with the performance of the Services under this Agreement. Voya shall obtain prior written consent from Client for services provided specifically for the Client and not for Voya on an enterprise-wide basis (e.g., printing and mailing). Voya has disclosed all subcontractors servicing the Plan at the time of entering into this Agreement. In all instances Voya shall remain responsible for the performance of any subcontractor.
- 14.2 Assignment.** Neither Party may assign any of its rights under this Agreement without the prior written consent of the other Party, which consent shall not be unreasonably withheld or delayed. Subject to the foregoing, all of the terms and provisions of this Agreement shall be binding upon and inure to the benefit of and be enforceable by the successors and permitted assigns of Client and Voya.

## 15. SUSPENSION OF SERVICES

Voya reserves the right to suspend all or any portion of the Services for a period not to exceed 48 hours per suspension to conduct routine servicing and maintenance of the facilities of Voya and/or its subcontractors. Voya will endeavor to suspend Services only during weekends to the extent reasonably practicable so as to minimize service interruption but reserves the right to extend the suspension into the hours prior to the New York Stock Exchange's opening on the next business day following the weekend in connection with significant system release activities.

## 16. NOTICES

All notices, requests, demands and other communications required to be given hereunder shall be in writing and shall be deemed to have been duly given on the earlier of the day of delivery by hand or telephonic facsimile (duly receipted), or the day after sending by recognized overnight courier service or five (5) days after mailing, certified or registered mail, return receipt requested, or electronically in each case to the Party for whom intended at the address specified in this Section.

If to Voya:

Voya Institutional Plan Services, LLC  
30 Braintree Hill Office Park  
Braintree, MA 02184  
Attn: Legal Department

If to Client:

Office of Finance & Treasury (OFT)  
1101 4<sup>th</sup> Street S.W., Suite 850W  
Washington, D.C. 20024  
Attn: Rodney Dickerson

## 17. REPRESENTATIONS

- 17.1 **Corporate Authority and Due Execution.** Each Party represents that (i) it has the power and authority to execute, deliver and perform this Agreement and that the execution, delivery and performance of this Agreement have been duly authorized by all necessary action of its members, and (ii) this Agreement constitutes a legal, valid and binding obligation enforceable in accordance with its terms.
- 17.2 **Plan Expenses.** Client represents that neither the sponsor of the Plans nor any affiliate of such sponsor is obligated to pay the expenses of the Plans with respect to the Services.

## 18. RELATIONSHIP OF THE PARTIES

- 18.1 **General.** The relationship between the Parties is that of independent contractors. None of the provisions of this Agreement shall be construed to create an agency, partnership or joint venture relationship between the Parties or the partners, officers, members or employees of the other Party by virtue of either this Agreement or actions taken pursuant to this Agreement.
- 18.2 **Fiduciary Status.** Except with respect to, solely, any qualified domestic relations order services provided to the Plans by Voya, Client and Voya intend that Voya shall not perform any service that would cause to be a fiduciary, within the meaning of ERISA, the Investment Advisers Act of 1940, or any state law, with respect to any Plan. Voya shall not have any discretion with respect to the management or administration of any Plan or with respect to determining or changing the rules or policies pertaining to eligibility or entitlement of any Participant in any Plan to benefits under such Plan. Voya also shall not have any control or authority with respect to any assets of any Plan, including the investment or disposition thereof. All discretion and control with respect to the terms, administration or assets of any Plan shall remain with Client or with the named fiduciaries under such Plan.

Client acknowledges that the Plan's authorized fiduciary is responsible for the selection of service providers and investment options and that (i) Client is a fiduciary, within the meaning of ERISA, with respect to the Plans; (ii) Client is independent in all respects of Voya and all affiliates of Voya; and (iii) Client has not relied on any advice or recommendation of Voya or any affiliates of Voya as a primary basis for making the decision to enter into this Agreement or with respect to the selection of particular investment options for any Plan.

## 19. GENERAL PROVISIONS

- 19.1 **No Waiver.** A Party's failure at any time to enforce any of the provisions of this Agreement or any right with respect thereto shall not be construed to be a waiver of such provision or right, nor to affect the validity of this Agreement. The exercise or non-exercise by a Party of any right under the terms or covenants herein shall not preclude or prejudice the subsequent exercise of the same or other rights under this Agreement.

- 19.2 Severability.** The terms and provisions of this Agreement shall be severable. If any term or provision is held to be invalid or unenforceable, that term or provision shall be ineffective to the extent of such invalidity or unenforceability and the remaining terms and provisions shall continue in full force and effect.
- 19.3 Entire Agreement.** Subject to the terms and conditions hereof: (i) this Agreement together with its exhibits, schedules, and attachments contains the entire understanding of the Parties with respect to the provision of the Services; (ii) there are no expectations, restrictions, promises, warranties, covenants, or undertakings other than those expressly set forth herein; and (iii) this Agreement supersedes all prior agreements and understandings between the Parties with respect to the Services. Notwithstanding this Section 19.3, this Agreement includes and incorporates by reference the materials included in the Solicitation, Offer, and Award for this Agreement. To the extent the terms in the Solicitation, Offer, and Award contradict any provision included in this Agreement, the standards in the Solicitation, Offer, and Award shall take precedence.
- 19.4 No Third Party Beneficiaries.** This Agreement is for the benefit of the Parties and their respective successors and permitted assigns. It is not intended to create a benefit to any third parties.
- 19.5 Governing Law.** This Agreement shall be governed by and interpreted and enforced in accordance with the laws of the District of Columbia, without regard to the conflict of laws provisions thereof, except that when federal law exists on substantive matters requiring construction under this Agreement, such federal law shall apply in lieu of state law but only to the extent required by applicable federal laws.
- 19.6 Survival of Obligations.** The Parties' respective obligations under this Agreement which by their nature would continue beyond the termination or expiration of this Agreement, including, without limitation, those contained in the Sections entitled Compensation, Confidential Information, and Indemnification shall survive the termination or expiration of this Agreement.
- 19.7 Headings and Captions.** All headings and captions contained in this Agreement are for convenience of reference only and shall not affect in any way the interpretation or meaning of this Agreement.
- 19.8 Pronouns.** Words used herein, regardless of the number and gender specifically used, shall be deemed and construed to include any other number, singular or plural, and any other gender, masculine, feminine, or neuter, as the context requires.
- 19.9 Counterparts.** This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.



IN WITNESS WHEREOF, the Parties hereto have duly executed this Agreement effective as of the date first above written.

**VOYA INSTITUTIONAL PLAN SERVICES, LLC**

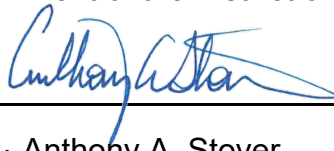


By: \_\_\_\_\_

Name: Gavin Gruenberg

Title: Vice President

**Government of the District of Columbia**



By: \_\_\_\_\_

Name: Anthony A. Stover

Title: Contracting Officer

**EXHIBIT A**

**PLAN PROVISIONS AND SERVICES REQUIREMENTS DOCUMENT**

***[Insert or attach Plan Provisions and Service Requirements Document]***

## EXHIBIT B COMPENSATION SCHEDULE

*Refer to final fee schedule dated September 4, 2024*

**EXHIBIT C**

**LIST OF PLANS**

1. District of Columbia 457(b) Deferred Compensation Plan
2. District of Columbia 401(a) Defined Contribution Plan
3. Not for Profit Hospital Deferred Compensation Plan
4. Not for Profit Hospital 401(a) Defined Contribution Plan

## EXHIBIT D

### SERVICE STANDARDS

Voya and Client have identified certain minimum performance standards as detailed in this Exhibit ("Service Standards"). Service Standards shall be applicable only to the extent all material information necessary for the successful delivery of Services subject to the Service Standards is received by Voya in "Good Order" (as such term is defined below). Voya's payment of any Service Standard penalties and/or waiver of any fee amounts otherwise payable to Voya shall not constitute an admission of liability or violation of applicable law and shall reflect, solely, a contractual obligation as provided in this Agreement and Exhibit.

For all purposes of this Exhibit, Voya's performance is subject to "Good Order." "Good Order" means Voya's receipt of necessary and required data, information, approvals and authorizations that conform to Voya's reasonable instructions, as mutually agreed by the parties, regarding the timing, form and method of transmission of information, consents or assets relevant to the various services.

Voya has agreed to place at risk a total of up to 20% of the fees it receives on a quarterly basis for the daily valuation of the Plans (as described in Exhibit B, the Fee Schedule) for not meeting the service standards set forth below as allocated across those standards via the "percentage of at-risk fees" column. The Forfeited amounts will be measured and calculated quarterly. For example, any penalties occurring during the second quarter will be calculated and applied collectively on the July invoice. Voya will provide Client with quarterly reporting concerning performance against the various service standards where available.

The first quarterly measurement period shall begin on [INSERT DATE].

Transaction	Timing standard	Amount at risk for missing standard
Issuance of Participant Statements	99% mailed / posted to the web within 15 business days following quarter end.	*
Transaction Confirmation Statements	98% mailed within two business days after processing.	*
Plan Sponsor Administrative Reports (Electronic copies)	100% provided within five business days, most within one day. For complex reporting requests, the time frame will be mutually agreed upon between the District and Voya.	*
Processing Payroll Contributions	Files received in good order prior to the close of the NYSE must be processed within two business days of receipt.	*

Processing New Loans	Requests received in good order prior to the close of the NYSE must be processed within two business days of receipt.	*
Hardship/Unforeseen Emergency Withdrawal Requests	Requests received in good order prior to the close of the NYSE must be processed the same day received.	*
Termination/Rollovers/Direct Transfers for Distribution	Requests received in good order prior to the close of the NYSE must be processed the same day received.	*
Fund Balance Transfers	Requests received in good order prior to the close of the NYSE must be processed the same day received.	*
Investment Election Requests	Requests received in good order prior to the close of the NYSE must be processed the same day received.	*
Error Corrections and Adjustments	Voya will promptly notify the District after becoming aware of an error resulting from the acts or omissions of Voya, Voya's computer system malfunctions, its staff errors or otherwise caused by Voya's negligent acts. Voya will make a good faith effort to correct any such error as soon as reasonably practicable after identification of the error and, where applicable, the District's determination or approval of the correction to be applied to such error.	*

Contribution Percentage Elections/Changes	Requests received in good order prior to the close of the NYSE must be processed the same day received.	*
QDRO Processing	99% of QDRO requests received by the close of the NYSE will be processed within five business days of receiving all required supporting documentation in good order. If the account contains a SDBA, the standard is within seven business days.	*
Setting an Appointment with an Onsite Representative	Our sophisticated scheduling tool makes setting up an appointment simple and easy. Employees can add as much relevant information as desired for the meeting.	*

\*Voya will place up to 20% of our fees at risk for not meeting the service standards we agree upon during the implementation process. The percentage is mutually agreed upon and may be broken out by the metrics most important to the District. If, for any reason, we do not meet either our timeliness or quality goal for any deliverable, we will clearly indicate within the Service Review what caused the problem and what course of action we are taking to avoid any such future occurrence.

In addition, Voya guarantees a smooth and seamless transition to the Voya program and are willing to offer a \$200,000 implementation guarantee. We will work with the District to establish a mutually agreeable guarantee for the implementation. Our success is measured by ensuring that each step of the implementation process is monitored and delivered on time and that the District and plan participants are satisfied with our services. If Voya fails to resolve any deficiency within 30 days regarding the implementation, the District may request the service guarantee be paid.

## EXHIBIT E

### **VOYA 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.

Other capitalized terms used but not defined in this Exhibit E have the meanings given them in the Agreement.

#### **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
  - (iii) 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 E-1. Voya represents and warrants that, as of the Effective Date, the statements in Exhibit E-1 are true and correct in all material respects.

### **3. Privacy and PI.**

- 3.1. With respect to any PI, Voya will:
- (a) Comply with the Voya Privacy Notice at [www.voya.com/privacy-notice](http://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:

<b>MEDIUM</b>	<b>DESTRUCTION METHOD</b>
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 E-1

### Security Requirements

<b>FC: Foundation Controls</b>	
<b>FC-1: Information Asset Management</b>	
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.
<b>FC-2: Data Privacy and Confidentiality</b>	
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.
<b>FC-3: Configuration Management</b>	
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.
<b>FC-4: Operating Procedures and Responsibilities</b>	
FC-4.1	<p>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.</p> <p>Voya IT policies and standards document the policies and procedures for job scheduling processes and tools.</p>

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.
<b>FC-5: Security Awareness and Training</b>	
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.
<b>UA: User Access Controls</b>	
<b>UA-1: User Access Controls</b>	
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.
<b>UA-2: Access Control Management</b>	
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.
<b>UA-3:</b>	<b>User Access Management</b>
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:
<b>UA-4:</b>	<b>Information Access Restriction</b>
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.
<b>PS:</b>	<b>Platform Security Controls</b>
<b>PS-1:</b>	<b>Computer System Security (Servers and Multi-user Systems only)</b>
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.
<b>PS-2: Network Security</b>	
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.
<b>PS-3: Generic Application and Database Security</b>	
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.
<b>PS-4: Workstation and Mobile Devices Security (End User Devices)</b>	
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.
<b>PS-5: Backup and Restore</b>	
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.
<b>PS-6: Remote Network Access Controls</b>	
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.
<b>ITR: IT Resilience Controls</b>	
<b>ITR-1: Architecture</b>	
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.
<b>ITR-2: Hardware and Software Infrastructure Resilience</b>	
ITR-2.1	<p>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:</p> <ul style="list-style-type: none"> <li>• Identified and cataloged</li> <li>• Supported by the manufacturer of the component (or if developed in-house, follows Voya's SDLC Policy which includes quality/security)</li> <li>• Applications and systems classified as A4 may be designed with high availability features and have no single point of failure</li> <li>• Reviewed on a regular basis for capacity implications (at minimum once every 12 months)</li> </ul>
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.
<b>ITR-3: Capacity Assurance</b>	
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.
<b>CM: Change Management Controls</b>	
<b>CM-1: Change Management Process</b>	
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.
<b>CM-2: Separation of Environments</b>	
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- production environments.
<b>SM: Security Monitoring Controls</b>	
<b>SM-1: Security Event Monitoring and Incident Management</b>	
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.
<b>SM-2: Technical State Compliance</b>	
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.
<b>SM-3: Security and Penetration Testing</b>	
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.

## EXHIBIT F

### RECORDKEEPING EXPENSE ACCOUNT PROCEDURES

1. Voya shall deposit an amount equal to the Fund Revenue that it receives from the Funds (excluding assets in SDBAs, company stock funds or participants loans) into the Recordkeeping Expense Account established for the Plan. Fund Revenue shall be available to pay any qualified ERISA expenses for the administration of the Plan as determined by the Client and/or be allocated to Participant accounts upon written direction from Client.
2. Voya shall deposit amounts equal to the Fund Revenue into the Recordkeeping Expense Account promptly after the completion of its standard receivables reconciliation process. Fund Revenue will normally be received by Voya from a Fund on a monthly or quarterly basis.
3. The assets held within the Recordkeeping Expense Agreement will be invested in a designated investment alternative available under the Plan pursuant to written direction received by Voya from Client.
4. Client agrees that all amounts deposited into the Recordkeeping Expense Account during a calendar year must be expended to pay qualified ERISA expenses and/or allocated to Participant accounts by March 31<sup>st</sup> (or the preceding business day) of the succeeding year.
5. It shall be the sole responsibility of Client to determine whether expenses are properly payable from the Recordkeeping Expense Account. For those expenses that Client has determined to be paid from the Recordkeeping Expense Account, Client will request payment from Voya for the amount of the expense using the applicable Plan Sponsor Expense Certification Template Letter included in this Exhibit and will certify the following to Voya in such letter relative to each requested payment:
  - a) The Plan document does not prohibit the payment of the expense;
  - b) The expense is related to the fiduciary's administration of the plan and not related to the Plan sponsor's "settlor" function; and
  - c) The expense is necessary, prudent and for a reasonable amount.

Further, if an expense is for services provided by a party-in-interest to the Plan, the Plan Client shall represent that the service is necessary for the operation of the Plan and is furnished under an arrangement for reasonable compensation.

6. Within ten (10) business days of Voya's receipt of the Plan Sponsor Certification Letter, Voya shall make a payment of the amount requested. Client may direct Voya to make such payment directly to a service provider or may direct Voya to reimburse the Plan for amounts that the Plan has previously paid (e.g., from its forfeiture account).

**Plan Sponsor Expense Certification Template Letter**  
**(for direct reimbursement)**

[Date]

[Name]

Voya Institutional Plan Services, LLC  
30 Braintree Hill Office Park  
Braintree, MA 02184

Re: Expense Reimbursement Certification

Dear [Name]:

Pursuant to of the Administrative Services Agreement ("Agreement") between [CLIENT NAME] ("Client") and Voya Institutional Plan Services, LLC ("Voya"), and in my capacity as a fiduciary under the [NAME OF PLAN] (the "Plan"), this letter is to direct you to reimburse Client in the amount of \$\_\_\_\_\_ representing expenses for services incurred by Client as plan administrator of the Plan. Client represents that the expense (i) relates to the fiduciary's administration of the plan; (ii) is prudent and for a reasonable amount; and (iii) the payment of such expense is not prohibited under the terms of the Plan document. Furthermore, if the expense is for services provided by a party-in-interest to the Plan as that term is defined under the Employee Retirement Income Security Act of 1974, then Client warrants that the service is necessary for the operation of the Plan and furnished under an arrangement for reasonable compensation. This instruction shall constitute Client Direction as defined under the Agreement between Client and Voya.

Sincerely,  
[Signature]

Name: \_\_\_\_\_

Title: \_\_\_\_\_

**Plan Sponsor Expense Certification Template Letter**  
**(for third-party payment)**

[Date]

[Name]

Voya Institutional Plan Services, LLC  
30 Braintree Hill Office Park  
Braintree, MA 02184

Re: Expense Reimbursement Certification

Dear [Name]:

Pursuant to of the Administrative Services Agreement ("Agreement") between [CLIENT NAME] ("Client") and Voya Institutional Plan Services, LLC ("Voya"), and in my capacity as a fiduciary under the [NAME OF PLAN] (the "Plan"), this letter is to direct you to pay a third party service provider to the Plan (as identified in the attached invoice) in the amount of \$\_\_\_\_\_ representing expenses for services provided to the Plan. Client represents that the expense (i) relates to the fiduciary's administration of the plan; (ii) is prudent and for a reasonable amount; and (iii) the payment of such expense is not prohibited under the terms of the Plan document. Furthermore, Client warrants that the service is necessary for the operation of the Plan and furnished under an arrangement for reasonable compensation. This instruction shall constitute Client Direction as defined under the Agreement between Client and Voya.

Sincerely,  
[Signature]

Name: \_\_\_\_\_

Title: \_\_\_\_\_



## EXHIBIT G

### POLICY FOR CORRECTION OF INADVERTENT PROCESSING ERRORS

As your plan's administrative service provider, Voya Institutional Plan Services, LLC ("Voya") has agreed to process transaction orders received in good order prior to market close from the plan and plan participants, alternate payees and beneficiaries (collectively, "Participants") accurately and on a timely basis. Voya seeks to avoid transaction processing errors to the greatest extent possible, but inadvertent errors do occur from time to time. Inadvertent processing errors are exclusively defined as incorrect or untimely processing by Voya employees of transactions that are received in good order. Inadvertent processing errors do not include errors made by plan sponsors or third parties.

Voya will correct any identified inadvertent processing error caused by Voya (a "Voya inadvertent processing error") as soon as reasonably practicable after identification of the error and, where applicable, the plan fiduciary's determination or approval of the correction to be applied to such error. Voya represents that in no event will Voya exercise discretionary authority or control over the correction of inadvertent processing errors in order to maximize gain or correct such error for Voya's own benefit or interest.

Once a Voya inadvertent processing error has been identified, Voya will promptly take corrective action to put the plan and its Participants in a position financially equivalent to the position they would have been in if the processing error had not occurred. This means that Voya will make the plan whole for any loss to the plan resulting from correcting a Voya inadvertent processing error. If any gain to a plan results in connection with a corrected transaction, Voya will keep that gain. The following examples illustrate the effect of the policy:

When a plan Participant directs that a certain dollar amount be contributed to his or her plan account, Voya credits the number of investment units that dollar amount will purchase to the Participant's account on Day 1, the day the contribution is processed. The number of units is based on the unit's dollar value on Day 1, as set by the investment fund and communicated to Voya after market close. If an inadvertent error occurs, and Voya does not process the contribution until Day 2, Voya will determine the number of units that should have been credited on Day 1, using Day 1's unit price. If, on Day 2, the unit price has gone up, the dollar amount of the contribution will not be enough to cover the number of units the Participant should have received. Voya will make up the difference such that the Participant receives the number of units he or she would have received on Day 1 and Voya will absorb the loss. The Participant is not charged for any additional cost. However, if, on Day 2, the unit price has gone down, the amount of the contribution would purchase more units on Day 2 than it would have purchased on Day 1. In that circumstance, the Participant will receive the number of units he or she would have received on Day 1 had the transaction been processed and Voya will keep the excess as part of its overall fee for services under its contract. Regardless of whether there is a gain or a loss, the Participant receives the benefit of what he or she requested.

When a plan Participant makes a withdrawal request of a certain dollar amount from his or her account, Voya liquidates or sells the number of investment units needed in order to make the distribution. Thus, on Day 1, Voya typically would sell or liquidate investment units in the Participant's investment fund at Day 1's price to make the distribution. If, due to a Voya inadvertent processing Error, Voya processes the instructions a day late, Voya will make sure that the Participant receives the dollar amount he/she requested. Voya will sell or liquidate the

same number of units that would have been sold on Day 1 had the transaction been accomplished on Day 1. If the unit price has declined, liquidated units will have a lower value on Day 2 than they had on Day 1, which means that Voya must make up the difference so that the Participant receives the requested amount in full. In doing so, Voya will incur a loss, which it absorbs. On the other hand, if the market has gone up and the units have increased in value, Voya will sell the same number of units as it would have sold on Day 1, but the sales amount will be higher than the requested withdrawal. Voya will keep the excess as part of its overall fee. In either circumstance, the Participant receives the benefit of what he or she requested and bears no additional cost.

Voya tracks the net financial experience and the effect of the corrections for each affected plan on an annual basis and will make that information available in accordance with ERISA Section 408(b)(2). Any gains kept by Voya constitute additional compensation for the services provided by Voya under its contract.