AON

HUMAN CAPITAL SOLUTIONS AT AON
SERVICES AGREEMENT

The Human Capital Solutions practice at Aon (which delivers products and services under the Aon, McLagan, Radford, Gauge and Client Insight names) provide a broad range of compensation and rewards and performance benchmarking, analytics, survey and consulting services.

This Human Capital Solutions Services Agreement (this "**Agreement**"), effective as of the date electronically approved or signed, is made and entered into by and between **State Board of Administration of Florida** ("**Client**") and **Aon Consulting, Inc. and its Affiliates** ("**Aon**" and, together with Client, the "**parties**").

Whereas, Client has selected Aon to provide certain of Aon Human Capital Solutions surveys, studies, products and consulting services, and Aon is willing to provide such services upon the terms and conditions contained in this Agreement. The parties agree to the following terms and conditions:

1. **Definitions.** As used in this Agreement, the following terms shall have the meanings set forth below:

a. "**Affiliates**" means an entity which is controlled by, controlling or under common control with Aon or Client respectively.
b. "**Approved User**" means any Client employee approved by Client to use or access the Services or Site.
c. "**Approved Consultant**" means any third-party individual or entity that obtains any Aon Confidential Information for the purpose of performing services for Client.
d. "**Client Data**" shall mean the information provided by Client necessary for Aon to perform the Services.
e. "**Confidential Information**" includes information of a business, compensation, or financial nature which one party discloses (the "Disclosing Party") to the other party (the, "Receiving Party") and is designated as being confidential or that a reasonable person would consider, from the nature of the information and circumstances of disclosure, as confidential to the Disclosing Party, including, but not limited to Client Data, Deliverables (including information contained in survey/benchmark reports), company memoranda, documents, diagrams, data, and/or software provided by the Disclosing Party. Confidential Information does not include information which: (i) is or becomes generally available or known to the public through no fault of the Receiving Party; or (ii) has already been or is hereafter independently acquired or developed by the Receiving Party without violating any confidentiality agreement with or other obligation to the Disclosing Party.
f. "**Deliverables**" means the results of the Services (including survey results, reports, processed data or other information or materials), written advice, letters and/or other advisory materials provided as part of the Services.
g. "**Services**" means the benchmarking surveys, studies, products, and consulting services to be performed by or on behalf of Aon as further described in a Statement of Work attached to, or entered into pursuant to, this Agreement.
h. "**Site**" will mean the website controlled by Aon through which certain Services may be accessible or Deliverables provided.
i. "**Statement of Work**" shall mean a supplement to this Agreement that particularly describes the Services to be furnished by Aon, the fees for such Services, and any additional terms and conditions pertaining thereto.

2. **Fees and Expenses.** The fees set forth in the applicable Statement of Work shall be payable within thirty (30) days of the invoice date. If no specific written fee applies, the fees will be calculated with reference to the time spent by Aon, using our prevailing standard hourly rates for each category of staff and unless otherwise agreed Aon will bill Client monthly. Aon will invoice Client via email, and all payments will be made via electronic payment. Client shall pay all reasonable pre-approved travel and related living expenses incurred by Aon's personnel in performing Services. Aon reserves the right to charge interest on undisputed past due invoices at a rate up to 9% per year until payment is received.. Client is responsible for any and all taxes, however designated, that are levied or based on this Agreement, the charges stated in this Agreement, or the Services or their use, excluding taxes based on the net income of Aon.

3. **Client Responsibilities.**

a. Client agrees to submit on-time, complete, up-to-date and accurate Client Data in accordance with Aon's instructions as necessary for the Services. If the Client Data submission is late or incomplete, Deliverables may be suspended until the Client Data is received.

b. A password will be assigned to each Approved User for access to the Site, if applicable. Client will provide Aon with a list of its individuals to be enabled as Approved Users. Aon will disable passwords for any current Approved User upon request. Client and Approved Users will not share passwords without the express written consent of Aon. Any unapproved use of or access to the Site, is prohibited, and will terminate any permission or license granted under this Agreement to use the Site, and the Services.
c. If Client desires to use a data entry contractor solely to provide Client Data to Aon on behalf of Client, Client will enforce this Agreement with such contractor, and will require the contractor to destroy any Aon Confidential Information the contractor received when its services to Client are complete.
d. If Client desires to provide Aon Confidential Information to an Approved Consultant, at Aon's discretion, the Approved Consultant must first enter into a non-disclosure agreement provided by Aon. Client agrees that Aon may share this Agreement and any applicable Statement of Work with the requested Approved Consultant. Aon reserves the right to deny or terminate access of an Approved Consultant at any time, and Client will cease providing Aon Confidential Information to such Approved Consultant upon notice.

4. **Confidential Information and Personal Data**

a. Each party will use reasonable efforts to cause its employees to minimize distribution and duplication and prevent unapproved disclosure of Confidential Information.
b. Aon and its Affiliates may use Client Data to produce reports, analysis, or results for services and disclose them to: Aon Affiliates, employees, agents, subcontractors, counsel and auditors; Client; and other Aon customers provided that such Client Data is aggregated and is not individually identifiable. Due to the continued use of data in active and archival surveys, Client Data will not be returned or destroyed and will be retained in accordance with Aon's corporate record retention schedules.
c. Subject to Section 3(d) and Section 4(d), Client and its Approved Users may only disclose Aon Confidential Information to Affiliates for which Client Data has been submitted, Approved Consultants and the employees of such entities with a need to know such Aon Confidential Information. Client and its Approved Users will not disclose or make available Aon Confidential Information, including Aon Confidential Information contained in the Deliverables, to any other Client Affiliates, or to any other third party.
d. Where Client or Approved Users disclose any Deliverables to its Affiliates, Client shall procure:
   a) the Deliverables are disclosed in full and no disclaimers are removed from the Deliverables prior to disclosure;
   b) that all such recipients accept such Deliverables: (i) on the basis Aon's aggregate liability, collectively, to those recipients and Client is no greater than our aggregate liability to Client as set out in this Agreement and (ii) subject to an obligation not to disclose such Deliverables to third parties, other than as required by law or court order.
e. Client agrees that Aon may disclose that Client and/or Affiliates are participants in an applicable survey. Survey participant lists may show general company information specific to Client/Affiliates, including some or all of the following: (i) company name; (ii) industry; (iii) headquarters location; (iv) company ownership (public/ private); and (ix) primary location and countries from which Client Data was submitted.

f. To the extent that any personal data is processed by the parties pursuant to this Agreement, then each Party will observe all applicable requirements of data protection laws and the data protection terms set forth in Exhibit A to this Agreement shall apply.
g. The parties agree that (i) Aon is not able to perform its obligations to Client under the Agreement unless Client provides personal data relevant to the Services, (ii) that such personal data is necessary to the performance of the Services in support of Client's business purposes as that term is defined under applicable law, and (iii) such personal data is not provided to Aon in exchange for any monetary or other valuable consideration from Aon to Client.
h. Confidential Information may be disclosed pursuant to a subpoena or other valid legal or administrative process, provided that the receiving party shall notify the disclosing party of such required disclosure and the disclosing party has had a reasonable opportunity to quash, modify or otherwise contest, such process (at the disclosing party's expense).

5. **Ownership and Licensing Rights.** Aon will retain all right, title and interest in and to all intellectual property rights

embodied in or associated with the Services and in and to any Deliverables posted or available through the Services, including copyrights, patents, and trademarks. If applicable, Aon hereby grants Client a paid-up, worldwide, non-transferable, and non-exclusive license to access and use the Site during the term of and only in accordance with this Agreement in order to provide Client Data and receive, use and copy the Deliverables. The Deliverables are copyrighted by Aon. Client is granted a perpetual, worldwide, paid-up, royalty-free, non-exclusive license to use and copy the Deliverables for Client's internal business purposes only. Client will not undertake, cause, permit or approve the modification, creation of derivative works, translation, reverse engineering, decompiling, disassembling or hacking of the Services or Deliverables or any part thereof; and will not remove, obscure, make illegible or alter any notices or indications of the intellectual property rights that are affixed on, contained in or otherwise connected to any Services or Deliverables or other Aon materials.

6. Term. The term of this Agreement shall continue in perpetuity until either party provides 30 days prior written confirmation of termination. The term of each SOW will be set forth therein. If Client terminates this Agreement or an applicable SOW, all unpaid undisputed fees and expenses will become immediately due and payable and no refunds or credits are provided. Client will dispute any fees without undue delay and in good faith.

7. Liability and Indemnification.

a. THE SERVICES ARE MADE AVAILABLE ON AN "AS-IS WHERE IS" BASIS WITHOUT WARRANTIES OF ANY KIND EITHER EXPRESS OR IMPLIED. CLIENT ACKNOWLEDGES THAT THE SERVICES AND THE CONTENT DO NOT CONSTITUTE OR SUBSTITUTE FOR LEGAL ADVICE.
b. AON'S TOTAL LIABILITY TO CLIENT AND ITS AFFILIATES RELATING TO THIS AGREEMENT AND SERVICES PERFORMED FOR CLIENT SHALL NOT EXCEED THE ANNUAL FEES PAID FOR SUCH SERVICES UNDER THE APPLICABLE STATEMENT OF WORK. IN NO EVENT WILL EITHER PARTY BE LIABLE FOR ANY INDIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL, LOSS OF PROFITS, GOVERNMENT FINES, OR OTHER SIMILAR DAMAGES, EVEN IF SUCH LOSS WAS REASONABLY FORESEEABLE OR A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES.
c. AON WILL INDEMNIFY AND DEFEND CLIENT FROM ANY CLAIMS, DAMAGES, LOSSES, AND EXPENSES (INCLUDING REASONABLE ATTORNEYS' FEES AND EXPENSES) THAT THE SITE OR SERVICES INFRINGE A THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS, UNLESS THE CLAIM IS BASED ON THE CLIENT'S ALTERATION OR MISUSE OF THE SITE OR SERVICES. SUBJECT TO AON'S INFRINGEMENT INDEMNITY OBLIGATION, CLIENT WILL INDEMNIFY AND DEFEND AON FROM AND AGAINST ANY AND ALL CLAIMS, DAMAGES, LOSSES, AND EXPENSES (INCLUDING REASONABLE ATTORNEYS' FEES AND EXPENSES) MADE BY CLIENT'S CURRENT AND FORMER EMPLOYEES, AFFILIATES, BENEFIT PLANS, AND OTHER PARTICIPANTS RELATED TO CLIENT'S USE OF THE SERVICES.
d. Aon will endeavor to make the Site available to Client's Approved Users 24 hours per day, 7 days per week, except during periods of scheduled or emergency maintenance.
e. Each party acknowledges that damages may be an inadequate measure of loss in the event of breach by the other party of this Agreement and accordingly in such event the non-breaching party shall be entitled to seek equitable remedies (including injunction or otherwise).

8. Miscellaneous.

a. This Agreement, the applicable Statements of Work, or fully executed amendments that may be presented to Client from time to time, constitute the entire agreement of the parties and supersede all previous oral or written negotiations and agreements relating to the subject matter of this Agreement. Each Statement of Work will be a separate agreement between Aon (or an Aon Affiliate) and Client (or a Client Affiliate). Only the entities that sign a Statement of Work shall be liable for their respective obligations under that Statement of Work. In the event any terms of any Statement of Work conflict with the terms contained in this Agreement, the terms in a Statement of Work shall prevail. Moreover, in the event of any conflict between the Agreement, any Statement of Work, and

the Data Protection Schedule, the Data Protection Schedule controls.

b. This Agreement will be construed and enforced in accordance with the laws of New York and the jurisdiction of the courts of New York to settle any dispute or claim that arises out of or in connection with this Agreement or its subject matter or formation (including non-contractual disputes or claims).
c. It is agreed that the parties' respective obligations that by their nature continue beyond the termination or expiration of this Agreement include, but are not limited to, those contained in Sections 4, 5, 7, and 8.
d. Neither party will be liable for inadequate performance to the extent caused by a condition (for example: natural disaster, act of war or terrorism, riot, labour condition, governmental action, and Internet disturbance) that was beyond the party's reasonable control.
e. If any part of this Agreement is found unenforceable, the remaining provisions will remain in full force.
f. There are no third-party beneficiaries to this Agreement.
g. This Agreement will be binding on the parties and their respective successors and assigns. Neither party may assign its rights or obligations hereunder without the prior written consent of the other party, except either party may assign its rights and obligations to an Affiliate.
h. Client agrees that Aon may provide Client with notices by email or regular mail.
i. The delay or failure to assert a right or to insist upon compliance with any term of this Agreement shall not constitute a waiver of that right or excuse a similar subsequent failure to perform any such term or condition.
j. Nothing in this Agreement shall be interpreted as placing the parties in an employment, partnership, joint venture or agency relationship and neither party shall have the right or authority to obligate or bind the other party on its behalf.
k. Client may access content and resources, compensation tools and compensation news (the "Content") through the Site for internal business purposes of Client only. Aon shall have the right to alter or remove such Content from the Site from time to time in its sole discretion, and such Content is provided on an "as is" basis.

This Services Agreement is agreed to on behalf of Client by:

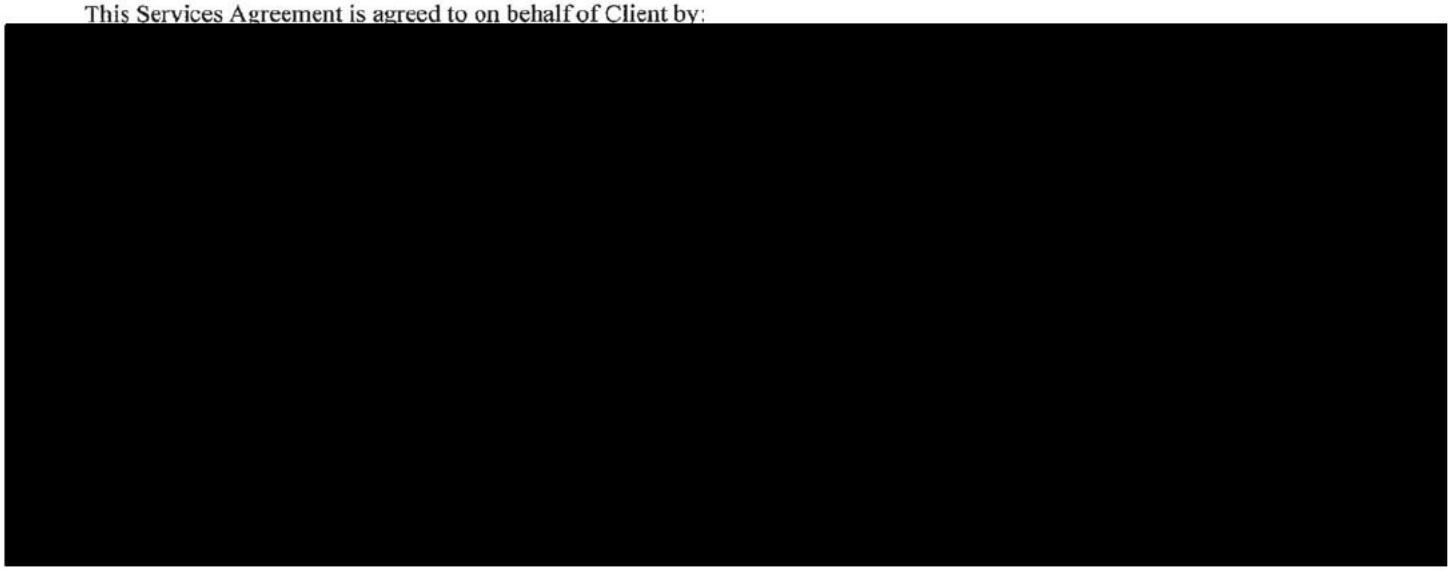

Exhibit A: Data Protection Schedule

This Data Protection Schedule ("**Schedule**") forms part of the Aon Human Capital Solutions Services Agreement ("**Agreement**") between Aon and Client and any applicable Statement of Work. To the extent that the provisions of this Schedule conflict with, or are inconsistent with, any provisions in the Agreement or any Statement of Work, the Schedule shall prevail.

1. **Definitions.** In this Schedule the following terms shall have the following meanings:

   a. "**Agreement Personal Data**" means any personal data (including any sensitive or special categories of data) that is transmitted, stored or otherwise processed under or in connection with the Agreement;
   b. "**Aon Group**" means the Aon group of entities worldwide, being Aon PLC, Aon's ultimate parent company, and all its subsidiaries, related/associated companies, Affiliates as well as joint ventures of such subsidiaries, related/associated companies and Affiliates;
   c. "**DP Laws**" means any applicable data protection and privacy laws relating to the protection of individuals with regards to the processing of personal data including but not limited to (i) the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"); (ii) the GDPR as transposed into the national laws of the United Kingdom ("**UK GDPR**"); (iii) Directive 2002/58/EC ("**ePrivacy Directive**"); (iv) the California Privacy Rights Act ("**CPRA**") and the California Consumer Protection Act of 2018 ("**CCPA**") and any corresponding or equivalent United States state or federal laws or regulations including any amendment, update, modification to or re-enactment of such laws (together "**US Privacy Laws**"); and (v) any corresponding or equivalent national or state laws or regulations including any amendment, supplement, update, modification to or re-enactment of such laws;
   d. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Agreement Personal Data;
   e. "**Restricted Transfer**" means a transfer of the Agreement Personal Data from the Client (or a Client Affiliate) to Aon (or Aon Affiliate(s)) which, in the absence of the SCCs, would be unlawful under DP Laws; and
   f. "**SCCs**" means (i) the standard contractual clauses set out in Commission Implementing Decision (EU)2021/914 for the transfer of personal data to third countries pursuant to GDPR, as updated, amended, replaced and superseded from time to time ("**EU SCCs**"); and the UK IDTA;
   g. "**UK IDTA**" means either the International Data Transfer Agreement (the "IDTA") or the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (the "UK Addendum") issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018.
   h. The terms "**controller**", "**data subject**", "**personal data**", "**processing**", "**processor**", "**sensitive personal data**", "**special categories of data**", "**supervisory authority**" and "**transfer**" shall have the same meanings ascribed to them under the DP Laws.
   i. Capitalised terms not defined in Section 1 shall have the meaning ascribed to them elsewhere in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

2. **Controller obligations**

   a. The parties envisage that under this Schedule each party is a separate controller of the Agreement Personal Data processed for the provision of the services applicable to the Agreement listed in Appendix 1 ("**Controller Services**").
   b. If the parties or their Affiliates (as applicable) enter into a Statement of Work, under which Aon agrees to provide services to Client which: (i) are listed in Appendix 1 then the relevant services shall be deemed applicable for the purposes of Appendix 1 from the date of that Statement of Work; or (ii) are not covered by Appendix 1, then the parties or their Affiliates (as applicable) may agree in writing to update Appendix 1 to insert details of the relevant services.
   c. Each party agrees for its own part that, to the extent that it processes Agreement Personal Data as

a separate controller, it will observe all applicable requirements of DP Laws and this Schedule in relation to its processing of Agreement Personal Data. Each Party shall notify the other in writing if it is no longer able to process Agreement Personal Data in accordance with DP Laws.

d. Aon and Aon Affiliates may process, transfer and disclose personal data as described in Aon's privacy notice in particular for (i) the delivery of the Controller Services; (ii) administration of engagement and general correspondence with Client; (iii) screening of individuals associated with Client against international sanctioned parties lists; and (iv) aggregation, de-identification and, where feasible, full anonymisation of personal data for benchmarking, market research and data analysis purposes associated with the development of Aon Group's products and services.
e. The parties will work together in good faith to ensure information prescribed by DP Laws is made available to relevant data subjects, which may include the Client's provision of such information to data subjects on Aon's behalf.

3. Security.

a. Each party shall implement appropriate technical and organisational security measures in relation to the processing of the Agreement Personal Data under or in connection with the Agreement, which shall ensure a level of security appropriate to the risk including, as appropriate, (i) pseudonymisation and encryption; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to the Agreement Personal Data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of those measures.
b. Aon shall maintain a global data governance framework which mandates strict technical and organisational security measures applicable to the processing of Agreement Personal Data including those relating to, without limitation, access control, data handling, malware protection, security organisation, system configuration and hardening, personnel security, physical security, business continuity plans and disaster recovery and third party security.
c. The parties shall each permit the other to take any reasonable and appropriate steps to ensure the parties process Personal Data in accordance with DP Laws

4. Mutual assistance.

a. If either party receives any complaint, notice or communication from a supervisory authority which relates to the other party's: (i) processing of the Agreement Personal Data; or (ii) potential failure to comply with DP Laws in respect of the Agreement Personal Data, that party shall direct the supervisory authority to the other party.
b. If a data subject makes a written request to a party to exercise any of their rights in relation to the Agreement Personal Data that concerns processing of the other party, that party shall direct the data subject to that other party.
c. To the extent applicable, the parties agree to cooperate to stop and remediate any actual or suspected unauthorized use of Personal Information.

5. Restricted Transfers.

a. With respect to Restricted Transfers, the SCCs are hereby incorporated into this Agreement by reference and will come into effect upon the commencement of any such Restricted Transfer, and the following terms shall apply. In each case, the data exporter is the Party or its Affiliates (as applicable) disclosing the personal data and the data importer is the Party or its Affiliates (as applicable) receiving the personal data.

(A) Where a Restricted Transfer is subject to the GDPR the following terms shall apply:
(i) Annex IA of the EU SCCs will be populated with the details of the Parties set out in the

Agreement, Annex IB of the EU SCCs will be populated with the description of processing of personal data set out in Appendix 1 of this Data Protection Schedule; and
(ii) For the purposes of Module 1 of the EU SCCs: clause 7 and the optional language in clause 11(a) shall not apply, the supervisory authority for the purposes of clause 13(a) shall be determined by the place of establishment of the data exporter, the governing law and choice of forum and jurisdiction stipulated in the Agreement shall apply to the extent that it is the law and the courts of an EU member state otherwise it shall be those of the Republic of Ireland, and the technical and organizational security measures set out in Section 3 herein shall apply. The frequency of the transfer shall be continuous, as necessary to deliver the Controller Services, and retention shall be determined by the corporate record retention schedules and policies of the relevant party.

(B) Where a Restricted Transfer is subject to the GDPR and the UK GDPR the following terms with respect to the UK Addendum shall, in addition to Section 5.a(A) above, also apply:
(i) the EU SCCs shall be read in accordance with, and deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the UK Addendum; and
(ii) the Parties confirm that the information required for the purposes of Part 1 (Tables) of the UK Addendum is set out in the Agreement.

(C) Where a Restricted Transfer is subject to the UK GDPR the Parties confirm that the information required for the purposes of Part 1 (Tables), Part 2 (Extra Protection Clauses) and Part 3 (Commercial Clauses) of the IDTA is set out in the Agreement and/or Appendix 1 of this Data Protection Schedule.

b. For the avoidance of doubt (and without prejudice to third party rights for data subjects under the SCCs) the parties hereby submit to the limitations stipulated in the Agreement with respect to their respective liability towards one another under the SCCs.
c. To the extent that there is any conflict or inconsistency between the terms of the SCCs and the terms of the Agreement, the terms of the SCCs shall take precedence.
d. If, and to the extent that, the European Commission or the United Kingdom issues any amendment to, or replacement of, the EU SCCs or the UK IDTA pursuant to Article 46(5) or Article 46 of the GDPR or UK GDPR, the Parties agree in good faith to take such additional steps as necessary to ensure that such replacement terms are implemented across all transfers.
e. If, at any time, a supervisory authority or a court with competent jurisdiction over a Party mandates that transfers from controllers in the EEA or the United Kingdom to controllers established outside the EEA or the United Kingdom must be subject to specific additional safeguards (including but not limited to specific technical and organisational measures), the Parties shall work together in good faith to implement such safeguards and ensure that any transfer of personal data is conducted with the benefit of such additional safeguards.

Appendix 1: Controller Services

Description of processing Where applicable, for the purposes of the SCCs the Agreement Personal Data is processed for the purposes of providing the Controller Services listed below and is processed for the duration of the Agreement. Processing operations may be set out more specifically in the Agreement and/or any applicable Statement of Work.			
Solution Line	**Service**	**Type of Personal Data**	**Categories of Data Subject**
Human Capital Solutions	**Rewards solutions and performance consultancy & Analytics solutions:** The rewards solutions and performance consultancy & analytics solutions practices provide benchmarking and trending analysis, advisory and consulting services across jobs, industries, markets and sectors on aspects including but not limited to: • industry focused compensation and company/performance metrics and insights • Designs for (executive /employee/sales/equity) compensation plans and equity valuations/reporting • Optimizing workforce (including sales force) productivity and performance • Corporate performance/ customer ratings • Managing people risk • Increasing workforce agility, diversity and resilience.	• Employee job titles and job descriptions. • Employee performance. • Education and professional experience. • Compensation data (for survey services), that may include, but not limited to the following: - Compensation Data in Local Currency. - Employee Work Location: Zip Code/Postal Code for Employees. - Unique employee identifier code or number (not to include employee name). • Optional to provide: Data revealing race or ethnic origin, health related information and reporting and sexual orientation related details where relevant to the services	Former, current and prospective employees of the Client, self-employed, contract personnel, secondees, temporary staff, agents, voluntary and casual workers, agent, or representative of, or any independent contractors working for the Client

Exhibit B – Security and Privacy of Personal Data

A. OVERVIEW

Aon acknowledges that, in the course of providing Services to Client pursuant to the terms of the Agreement, it may gain access to Personal Data (as defined below). Aon agrees to collect, process, transfer, disclose, store, and otherwise use Personal Data in the possession of Aon consistent with the terms of this Schedule, unless otherwise required by law.

This Schedule describes the general components of Aon's current data privacy and security programs. These programs are maintained by Aon to protect the confidentiality, security and integrity of Personal Data in the possession of Aon.

For purposes of this Schedule, **"Personal Data"** means an individual's name in combination with: (a) home or other physical address; (b) social security number or other similar government identifier; (c) health information; (d) financial account numbers in combination with a password, PIN, or security code that would permit access to the financial account; or (e) any other combination of data elements that would trigger individual or governmental notice under applicable law if exposed to an unauthorized third party.

Capitalized terms used but not defined in this Schedule shall have the meanings assigned to them in the Agreement. To the extent there is a conflict between the terms of this Exhibit B and Exhibit A, Exhibit A shall govern.

B. GENERAL REQUIREMENTS: DATA PRIVACY AND SECURITY

1. Data Privacy and Security Programs. Aon's data privacy and security programs shall include reasonable and appropriate physical, technical, organizational and administrative measures designed to protect against the unauthorized destruction, loss, access to or alteration of Personal Data in the possession of Aon.

2. Data Privacy and Security Policies. Aon shall maintain policies and standards for the protection of Personal Data that originate from industry frameworks and establish uniform security and privacy standards for Aon operations. Such policies shall be consistent with ISO27001/2 or another generally accepted industry standard that is applicable to Aon as a service provider. These policies shall include, but not be limited to, a Global Privacy Policy, a Global Information Security Policy, and applicable sub-policies or standards that flow down or accompany these policies. Aon shall abide by these policies, which shall outline the physical, technical, organizational and administrative measures by which Aon protects Personal Data. Upon Client's request, Aon shall provide to Client current copies of such policies.

3. Third Party Subcontractors. Aon shall be responsible for ensuring that its subcontractors who have Personal Data maintain data security and privacy programs which are at least as stringent as Aon own programs with respect to the applicable service to which such subcontractor has been engaged, and in accordance with generally accepted industry standards and practices. Aon shall maintain a risk management program focused on the identification, evaluation, and validation of a vendor's security controls.

4. On Boarding Process. The following measures are undertaken at the commencement of an individual's employment or engagement with Aon:

a. *Background Checks*. Each individual assigned to perform Services under the Agreement will have been subjected to a background check in accordance with Aon's background checking policies. Each candidate's background check report is closely reviewed in determining whether employment of a candidate is consistent with the safe and efficient performance of Services, taking into consideration any appropriate factors and applicable law.

b. *Training*. Aon has implemented and maintains a Data Privacy and Information Security awareness program. Upon joining Aon, employees with access to Personal Data will be given training on data security and privacy issues as part of their new hire orientation, including on Aon's current Information Security and Data Privacy Policies. Employees further agree in writing to perform his or her work according to Aon's policies, standards, and procedures regarding information security and privacy requirements. Subsequent annual training is required and is supplemented by numerous educational initiatives. Depending upon job function, certain employees receive specialized training and/or receive training on a more frequent basis.

C. SECURITY MEASURES

Aon maintains appropriate data protection and security measures for Personal Data. Such measures shall include, but shall not be limited to, the following:

1. Physical Security. Aon maintains appropriate security controls for entry points, holding areas, telecommunications areas, and cabling areas that contain information processing systems or media containing Personal Data. Set forth below are examples of such security controls:

    a. Access controlled and restricted by use of a defined security perimeter, appropriate security barriers, security cameras, entry controls and authentication controls, and access logs are to be maintained for a minimum of two (2) years;

    b. Where Aon ID cards are deployed, all personnel (i.e. employees, contractors, vendors, visitors) are required to wear some form of visible photo identification to identify themselves as employees, contractors, vendors, or visitors;

    c. Aon maintains a clear desk/clear screen policy;

    d. Aon employs idle-lock for unattended equipment designed to prohibit access and use by unauthorized individuals;

    e. Visitors to Aon's premises are required to be escorted at all times; and

    f. Where technically feasible and commercially reasonable, cameras and CCTVs are installed and monitored 24/7, and recordings of images are kept for 90 days.

2. Network Security Controls. Aon maintains the following network security controls and safeguards designed to prevent unauthorized access to Aon's network:

    a. Defense-in-depth design with perimeter routers, network switches and firewall devices and default deny-all policy to protect its Internet presence;

    b. Least privilege and authenticated access for network users and equipment;

    c. Internet- access is controlled by proxies and logged;

d. Remote network access is governed by two-factor authentication with a non-reusable password and only allowed from Aon-owned equipment that meets current corporate standards;

e. Intrusion detection system is deployed to monitor and respond to potential intrusions;

f. Real-time network events are logged and investigated using a security information event management tool;

g. Content filtering and website blocking using approved lists;

h. Wireless Access to the Network is limited to approved systems;

i. All wireless network devices follow the same policies and standards as wired devices;

j. Bridging of wireless and other networks, both wired and wireless, including the corporate network, is strictly prohibited; and

k. Rogue wireless access points are detected and disassociated with the corporate wireless network.

3. Platform Security Controls. Aon maintains the following security controls and safeguards designed to protect and prevent unauthorized access to Personal Data on various computing platforms and operating systems:

a. Configuration/Hardening standards are established, documented, reviewed and updated regularly;

b. Changes are approved and follow Aon's internal change control process;

c. Unauthorized hardware and software are prohibited from being installed;

d. Where technically feasible, a session is timed out after 15 minutes of inactivity;

e. Vendor-supplied defaults (accounts, passwords and roles) are removed during installation;

f. Services and devices that are not required by valid business needs are removed;

g. An anti-virus program with timely updates actively runs on servers and machines; and

h. Workstation and laptop configurations:

1) Only non-privileged account access is allowed; and

2) Full disk encryption and active firewall are installed on all laptops.

4. Application Security Controls. The following security controls and safeguards are designed to ensure the integrity and security of applications developed by Aon:

a. Defense-in-depth with the use of n-tier architecture provides separation and protection of data;

b. Application development follows a secure software development life cycle (SSDLC) that includes training, development, testing and ongoing assessments;

c. All changes to such applications are documented, reviewed, tested and approved before being implemented into production;

d. Application vulnerabilities and patches are identified, tested and remediated/installed in a timely manner; and

e. Development and testing environments must not contain any production data.

5. Data and Asset Management. To protect Aon's computing assets and the data contained within these assets, the following safeguards are in place:

a. Personal Data is protected with the use of encryption, or other appropriate technical, administrative and physical safeguards;

b. Regular backups of Personal Data are performed and stored in a location separate from the primary storage location;

c. Personal Data transmitted over public networks and on removable media are encrypted using current industry standards;

d. A data loss prevention tool governs end point data transfer activities, including the use of removable media and Internet uploads;

e. An inventory program is in place and monitored to control the installation, ownership and movement of hardware, software and communications equipment;

f. All physical media leaving Aon's custody must be encrypted, sanitized, destroyed, or purged of Personal Data to ensure that residual magnetic, optical, electrical, or other representation of data has been deleted, and is not easily recoverable, prior to leaving Aon's custody; and

g. Personal Data is compartmentalized or otherwise logically separated from, and in no way commingled with other information of Aon's or its other clients.

6. Access Control and Management. The following controls are designed to ensure proper identification and authorization of access to Personal Data:

a. Aon (i) monitors and logs both access and use of the Aon system to access Personal Data, and (ii) keeps a log of each unsuccessful attempt to access the Aon system that handles Personal Data;

b. Access to Personal Data is role-based with valid business reasons, and is periodically reviewed, confirmed and updated, and access that is no longer needed is removed promptly;

c. Unique logon ID and passwords must be used;

d. Strong passwords with minimum length, complexity and expiration requirements must be used;

e. Access is disabled after a limited of failed number login attempts; and

f. Previously used passwords must not be re-used.

7. Vulnerability and Patch Management. To identify and mitigate vulnerabilities that threaten Aon's ability to enforce the confidentiality, integrity, and availability of Personal Data, the following measures are put in place:

a. A vulnerability monitoring process that provides alerts or notifications of new fixes available, and the resulting timeframe for remediation;

b. Regular scanning enables identification and remediation of vulnerabilities promptly; and

c. Vulnerabilities are classified based on severity and are remediated based on predetermined service level expectations.

D. ASSURANCE TESTING

1. Annual Penetration Testing. Aon performs penetration tests on applicable Aon environments, including perimeter vulnerability testing, internal infrastructure vulnerability testing, and application testing. Upon Client's request, Aon shall provide a summary of process documentation and external assessment results to the extent applicable to the Services provided to Client.

2. HIPAA Assessment. Aon conducts a periodic assessment in accordance with the requirements of the U.S. Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"). To the extent applicable to the Services, Aon shall provide an annual summary of such HIPAA assessment activities upon Client's request.

E. DATA BREACH NOTIFICATION & INCIDENT RESPONSE

1. Notification. In the event that Aon discovers or is notified of a confirmed breach or a reason to believe a breach occurred of security that results in the unauthorized access, disclosure, or loss of Personal Data while such data is in the possession, custody or control of Aon ("**Data Breach**"), Aon shall promptly and without undue delay notify Client's Authorized Representative of such Data Breach.

2. Incident Management. In the event of a Data Breach, Aon shall (i) reasonably investigate the impact of such Data Breach, (ii) identify the root cause of such Data Breach, (iii) take reasonable and appropriate measures to remedy the Data Breach, and (iv) take reasonable and appropriate measures to prevent a recurrence of such Data Breach.

3. Incident Reporting. Upon Client's request, Aon will provide any of the following information that is known to Aon Authorized Representatives at such time: (i) the nature of the Data Breach, (ii) the Personal Data used or disclosed in the Data Breach, (iii) the measures Aon has taken or will take to mitigate any deleterious effect of such Data Breach, and (iv) any corrective action Aon has taken or will take to prevent future similar Data Breaches from occurring.

4. Incident Remediation. Aon agrees to be responsible for all reasonable costs incurred by Aon related to or arising from any such Data Breach, including but not limited to, forensic and investigatory costs incurred by Aon, as such may be reasonably required. In addition, Client may require Aon, at Aon's expense, to provide the following notices when such notice is reasonably necessary and practical under the circumstances: (a) notification to individuals, where such individuals have been impacted by the Data Breach; and (b) notification to governmental entities, where such notice to governmental entities is required by law or regulation.

F. PRIVACY AND SECURITY REGULATORY COMPLIANCE

1. Compliance with Data Privacy Laws and Regulations. Aon will comply with data privacy laws and regulations applicable to Aon in its capacity as a service provider.

2. Health Insurance Portability and Accountability Act. If the Agreement or the Services involve both a Client "Covered Entity" and "Protected Health Information" as such terms are defined in HIPAA, then, in addition to all other requirements of this Schedule, Aon and Client shall execute a HIPAA Business Associate Agreement ("**Business Associate**

Agreement"). In the event of any conflict between the terms of the Business Associate Agreement and this Schedule, the Business Associate Agreement will govern.

3. European Union("EU"), and United Kingdom ("UK"). If the Agreement or the Services involve the disclosure or transfer of Personal Data of a person covered by any of the Data Privacy Laws, then, in addition to all other requirements of this Schedule, Aon and Client shall execute the Model Clauses specified by the EU and United Kingdom for the onward transfer of Personal Data and other such contracts that may be required to comply with Data Privacy Laws ("Onward Transfer Clauses"). In the event of any conflict between the terms of the Onward Transfer Clauses and this Schedule, the Onward Transfer Clauses will govern. For purposes of this Section:

    a. "Data Privacy Laws" means any applicable data protection and privacy laws relating to the protection of individuals with regards to the processing of personal data including but not limited to (i) the General Data Protection Regulation (EU) 2016/679 ("GDPR"); the GDPR as transposed into the national laws of the United Kingdom ("UK GDPR") and implementations of any of the foregoing by the individual EU or EEA Member States and UK, all as amended from time to time.

    b. "Model Clauses" means (i) the standard contractual clauses set out in Commission Implementing Decision (EU) 2021/914 for the transfer of personal data to third countries pursuant to the GDPR as updated, amended, replaced and superseded from time to time ("EU SCCs"); and/or (ii) either the International Data Transfer Agreement (the "IDTA") or the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (the "UK Addendum") issued by the UK Information Commissioner under section 119A(1) Data Protection Act 2018.

4. Gramm-Leach Bliley Act. Aon shall comply with the Gramm-Leach-Bliley Act ("**GLBA**"), 15 U.S.C. § § 6801-6827 to the extent that Aon is subject to the GLBA in the provision of Services to Client.

5. PCI. To the extent that Aon collects, stores, transfers or processes payment card information, Aon acknowledges and agrees that it is responsible for the security of such payment card information and will comply with the relevant sections of the most current Payment Card Industry Data Security Standard, as propagated by the PCI Security Standards Council and updated or amended from time to time during the term of the Agreement.

6. Massachusetts Security Regulation. The technical and organizational security measures implemented by Aon to protect Personal Data shall be consistent and no less stringent than those referenced applicable laws and regulations, including, without limitation, the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth (201 CMR 17.00).

Addendum to the Human Capital Solutions at Aon Services Agreement between Aon Consulting, Inc. and the State Board of Administration of Florida

Notwithstanding anything to the contrary in the Human Capital Solutions at Aon Services Agreement (the "Agreement") or any amendments to the Agreement, the following provisions apply to the State Board of Administration of Florida (SBA) as an entity of the State of Florida, are incorporated by reference into the Agreement, and are agreed to by Aon Consulting, Inc. (Aon).

1. The SBA, as an entity of the State of Florida, is prohibited from entering into indemnification agreements unless expressly authorized by law. (See Florida Attorney General Opinion 99-56, dated September 17, 1999.) The SBA is also prohibited from entering into a limitation of remedies agreement unless otherwise authorized by law. (See Florida Attorney General Opinion 85-66, dated August 23, 1985.) The SBA agrees to any sections on [Indemnification and Limitation of Liability] to the extent allowable and enforceable under Florida law.

2. Notwithstanding any provision in any agreement between the parties, Aon acknowledges and agrees that the SBA is bound by the provisions of Chapter 119 (Public Records), Florida Statutes, and in the event of any conflict between Chapter 119, Florida Statutes, and the terms of any agreement between the parties, the provisions and procedures of Chapter 119, Florida Statutes, will prevail.

3. **IF AON HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO AON'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS AGREEMENT, CONTACT THE CUSTODIAN OF THE PUBLIC RECORDS AT:**

STATE BOARD OF ADMINISTRATION OF FLORIDA
POST OFFICE BOX 13300
TALLAHASSEE, FLORIDA 32317-3300
(850) 488-4406
SBAContracts_DL@sbafla.com

(The font size, bolding and text set forth above are required by s. 119.0701(2)(a), F.S.)

4. Consistent with the Florida Transparency in Contracting Initiative, the SBA posts certain operational contracts on its website, and this Agreement will be one of the agreements posted. Aon hereby agrees that the SBA is authorized to post this Agreement (including any amendments or addenda hereto) and a description of the content of the Agreement (including any amendments or addenda hereto) on the SBA's website. At the time of execution Aon may submit a redacted version of the agreement for these purposes.

5. In accordance with section 448.095(5), Florida Statutes, Aon shall register with and use, and shall cause any of its subcontractors to register with and use, the E-Verify system to verify

the work authorization status of all new employees of the contractor or subcontractor performing work within the United States. Aon acknowledges that the SBA is subject to and Aon agrees to comply with section 448.095, Florida Statutes, as amended from time to time, to the extent applicable.

6. This Agreement shall not be construed as a waiver (i) of the sovereign immunity of the State of Florida; (ii) a waiver of the State of Florida's rights under the 11th Amendment to the United States Constitution; or (iii) to a jury trial.

FOREIGN COUNTRY OF CONCERN ATTESTATION
(PUR 1355)

This form must be completed by an officer or representative of an entity submitting a bid, proposal, or reply to, or entering into, renewing, or extending, a contract with a Governmental Entity which would grant the entity access to an individual's Personal Identifying Information. Capitalized terms used herein have the definitions ascribed in Rule 60A-1.020, F.A.C.

Name of entity is not owned by the government of a Foreign Country of Concern, is not organized under the laws of nor has its Principal Place of Business in a Foreign Country of Concern, and the government of a Foreign Country of Concern does not have a Controlling Interest in the entity.

Under penalties of perjury, I declare that I have read the foregoing statement and that the facts stated in it are true.

[redacted]

STATE BOARD OF ADMINISTRATION
OF FLORIDA

1801 HERMITAGE BOULEVARD, SUITE 100
TALLAHASSEE, FLORIDA 32308
(850) 488-4406

POST OFFICE BOX 13300
32317-3300

RON DESANTIS
GOVERNOR
CHAIR

JIMMY PATRONIS
CHIEF FINANCIAL OFFICER

ASHLEY MOODY
ATTORNEY GENERAL

LAMAR TAYLOR
INTERIM EXECUTIVE DIRECTOR &
CIO

MEMORANDUM

Date: **June 11, 2024**

To: **Paul Groom**
Deputy Executive Director

From: **Lamar Taylor**
Interim Executive Director & CIO

Subject: **Delegation of Authority**

I will be out of the office from **12:00 p.m. on Wednesday, June 12, 2024 through 5:00 p.m. on Friday, June 14, 2024.** I hereby appoint **Paul Groom** as my designee to carry out the duties and responsibilities that have been delegated to me by the State Board of Administration/Executive Director.

Prior to carrying out these duties and responsibilities, **Paul** will consult and coordinate with Executive Service Staff and other employees of the State Board of Administration, as needed.

If, because of unforeseen circumstances, this absence from the office extends beyond **5:00 p.m. on Friday, June 14, 2024**, the delegate listed above will continue to be my designee as described above for a reasonable period thereafter.