**TERMS OF REFERENCE OF THE CCTL GAA**

**In relation to the Aon Bigblue Touch Group Pension Plan and Bigblue Touch 4life**

## Definitions

In this document, the following terms have the following meanings:

| | |
|---|---|
| **Aon** | means Aon UK Ltd |
| **Aon Policyholder** | means a Relevant Policyholder who is a member one or more of the Aon Schemes |
| **Aon Schemes** | means Bigblue Touch and Bigblue Touch 4life |
| **Bigblue Touch (BBT)** | means the Bigblue Touch Group Personal Pension Plan which includes workplace personal pension schemes and a scheme for individual members. |
| **Bigblue Touch 4life** | means the decumulation phase scheme associated with Bigblue Touch – Bigblue Touch 4life. |
| **CCTL** | means Capital Cranfield Trustees Limited |
| **COBS** | means the FCA Conduct of Business Sourcebook |
| **Decumulation phase** | means the period commencing when a member first starts to draw benefits, including using Flexi Access Drawdown, payment of an Uncrystallised Funds Pension Lump Sum in respect of part of their fund or such other method permitted by the Relevant Scheme |
| **FCA** | means the Financial Conduct Authority |
| **Firm** | means a Relevant Scheme provider who has appointed the CCTL GAA. In these terms of reference, it is Aon UK Limited (Aon). |
| **GAA** | means the Governance Advisory Arrangement |
| **PT** | means Professional Trustees of CCTL. Any PT who is part of a GAA must by fully APPT accredited |
| **Relevant Policyholder** | means a member of a Relevant Scheme who is or has been a worker entitled to have contributions paid by or on behalf of his employer in respect of that Relevant Scheme |
| **Relevant Scheme** | means a personal pension scheme or stakeholder pension scheme for which direct payment arrangements are, or have been, in place, and under which contributions have been paid for two or more employees of the same employer. |

## PART A: The Activities of the GAA and relationship with Firms

### 1. Duties and Responsibilities and Independence

1.1 The GAA shall act solely in the interests of Aon Policyholders in assessing and raising concerns about the value for money in the Aon Schemes.

1.2 The GAA confirms its independence from the Aon Schemes and that the GAA Chair is

independent of each of the Aon Schemes in accordance with COBS 19.5.3.(3).

## 2. Value for money

The GAA will assess the ongoing value for money for Aon Policyholders. As part of this, the GAA will assess:

- Whether the Aon Schemes' default investment strategies, and those during the decumulation phase, are designed and executed in the interests of Aon Policyholders and have clear statements of aims and objectives.
- Whether the characteristics and net performance of investment strategies, including those during the decumulation phase, are regularly reviewed by Aon to ensure alignment with the interests of Aon Policyholders and that the Firms take action to make any necessary changes.
- Whether Aon Schemes' core financial transactions, including payments made to members during the decumulation phase, are processed promptly and accurately.
- The level of charges borne by the Aon Policyholders, including charges made in transition to and during the decumulation phase.
- The direct and indirect costs incurred as a result of managing and investing, and activities in connection with the managing and investing of, the pension savings of the Aon Policyholders, including transaction costs.
- Whether the communications to Aon Policyholders are fit for purpose and properly take into account the Aon Policyholders' characteristics, needs and objectives.
- All of the above, together with other criteria applied as appriopriate, will take into account current regulation and legislation at the time of reportting.

## 3. Investment considerations

3.1 Since Aon has an investment strategy and makes investment decisions which could have a material impact on the Aon Policyholders' investment returns, the GAA will provide an independent consideration of, and report on, Aon's policies regarding:

- The adequacy and quality of Aon's policy in relation to Environmental, Social and Governance (ESG) financial considerations (including any TCFD and/or similar compliance commitments) and how these are taken into account in Aon's investment strategy or investment decision making.
- The adequacy and quality of Aon's policy in relation to non-financial matters and how these are taken into account in Aon's investment strategy or investment decision making.
- The adequacy and quality of Aon's policy in relation to stewardship.
- All of the above, together with other criteria applied as appriopriate, will take into account current regulation and legislation at the time of reportting.

3.2 The GAA will consider and report on the extent to which Aon has implemented its stated policies in relation to the considerations and matters referred to above.

3.3 When the GAA is considering the adequacy and quality of Aon's policies regarding ESG financial considerations, non-financial matters, stewardship or other financial considerations, the GAA will form a view as to whether:

- the policy sufficiently characterises the relevant risks or opportunities;
- the GAA considers that a policy seeks to appropriately mitigate those risks or take advantage of those opportunities;
- Aon's processes have been designed to properly take into account those risks or opportunities;

- the policy is appropriate in the context of the expected duration of the investment; and
- the policy is appropriate in the context of the main characteristics of the Aon Policyholders.

## 4. Publication of Information on costs and charges

4.1 The GAA will ensure the publication by 30 September each year, in respect of the previous calendar year, of the required administration charges and transaction costs information. This information must be available without charge on a publicly accessible website and must include the costs and charges for each default arrangement and each alternative fund that a member is able to select. It must also include an illustration of the compounding effect of the administration charges and transaction costs, based on prescribed assumptions, for a representative range of funds options that a member is able to select.

4.2 The GAA will ensure that all members of the Aon Schemes are provided with an annual communication setting out the most recent transaction costs and administration charges information that has been published, together with an explanation of how that information is relevant to the Aon Scheme member and how an Aon Scheme member can access the full costs and charges information described in paragraph 4.1 above, with a link to the website.

4.3 The GAA will set out the information in the annual communication in a manner that pays due regard to the purposes for which Aon Policyholders might reasonably use the information. The GAA will make the annual communication available on request to Aon Scheme members' spouses and civil partners, as well as persons within the application of the Aon Schemes and qualifying or prospectively qualifying for benefits under the Aon Schemes.

## 5. Raising and escalation of concerns

5.1 In relation to the GAA's remit of review, the GAA will raise with Aon any concerns it may have in relation to any of the matters it has assessed or considered, or where the GAA is unable to obtain or has difficulties obtaining from Aon the information it requires.

5.2 The GAA will escalate concerns as appropriate, to the FCA and/or alert Aon Policyholders, their employers and/or make its concerns public, where Aon has not, in the GAA's opinion, addressed those concerns satisfactorily or at all.

## 6. Duties of the Firm in relation to the GAA

The Firm shall:

- Take reasonable steps to ensure that the GAA acts and continues to act in accordance with its terms of reference.
- Take reasonable steps to provide the GAA with all information reasonably requested by the GAA for the purposes of carrying out its role.
- Provide the GAA with sufficient support and resources so that the GAA is properly able to carry out its duties in the GAA's remit of review.
- Have arrangements to ensure that the views of the Aon Policyholders can be directly represented to the GAA.
- Take reasonable steps to address any concerns raised by the GAA under its terms of reference.
- Provide written reasons to the GAA as to why it has decided to depart in any material way from any advice or recommendations made by the GAA to address any concerns it has raised.
- Take all necessary steps to facilitate the escalation of concerns by the GAA.
- Make available the GAA's terms of reference and the three most recent annual reports, in a way

appearing to the Firm to be best calculated to bring them to the attention of Aon Policyholders and their employers by placing them in an appropriately prominent and relevant position on the Aon Scheme website (https://bbt.tbs.aon.com/legal/Governance%20Advisory%20Arrangement) and by providing them on request to Aon Policyholders and their employers.

- Provide to the GAA administration charges and transaction cost information, setting out the costs and charges for each default arrangement and each alternative fund option the member is able to select.
- Organise a clear escalation process for the GAA to access a person at Aon holding an FCA Significant-Influence or designated senior management Function.
- Not unreasonably withhold from the GAA information that would enable the GAA to carry out its duties in the GAA's remit of review.
- Have arrangements for sharing confidential and commercially sensitive information with the GAA.
- Use best endeavours to obtain, and shall provide the GAA with, information on the costs incurred as a result of managing and investing, and activities in connection with the managing and investing of, the assets of the Aon Schemes, including transaction costs and information about costs and charges more broadly.
- Provide additional resources and support to the GAA where Aon asks the GAA to take on responsibilities in addition to those listed above, such that its ability to act within its terms of reference is not compromised.
- In relation to the Firm's agreed future threshold testing, review the continued appropriateness of the GAA over an IGC, having regard to the complexity and nature of the size of the take-up, or expected size of the take-up, complexity and nature of the Aon Schemes.

## 7. Conflicts of Interest

7.1 The GAA will act in the interests of Aon Policyholders both individually and collectively. This is known as Member Representation and the Firm will ensure is is signposted and communicated to members. The GAA will provide the contact details for the representation to be made directly to the GAA. Where there is the potential for conflict between the individual and collective interests, the GAA should manage this conflict effectively. The GAA is not required to deal directly with typical complaints from individual policyholders, but will receive from the Firm a summary of complaints in respect of the Aon Schemes as part of its investigation.

7.2 If Aon asks the GAA also to consider the interests of other members or clients, Aon should provide additional resources and support to the GAA such that the GAA's ability to act in the interests of Aon Policyholders are not compromised.

# Part B: Structure and Organisation of the GAA

## B1. Membership

1.1 The Members of the GAA for Aon (the Aon GAA Team) shall consist of:

- Andrew Cheseldine – Chair and PT
- Kevin Wesbroom – PT
- Chris Drifill – head of Governance, CCTL

.

1.2 The board of CCTL have ensured that the Aon GAA Team has sufficient collective expertise and experience to be able to make judgements on the value for money for the Aon Schemes. All

decisions relating to the discharge of its duties shall require the agreement of the two PTs on the GAA Team. CCTL will regularly review their performance and the Terms of Reference of the GAA and its members.

1.3 The GAA and Firm shall meet as necessary in order to discharge its duties. The GAA will take a formal record of key decisions or minutes. Meetings between the GAA and the Firm may take place in person or by telephone or video conference.

1.4 CCTL and the GAA will hold the Firm's shared confidential and commercially sensitive information as specified in the appended Supplier Security Schedule.

**B2. CCTL - Aon GAA Team Outputs**

2.1 The GAA will be responsible for the production of an annual report for the Aon Scheme's by end of September latest each year, in respect of the previous calendar year, which will set out:

- the GAA's opinion on the value for money delivered by the Aon Schemes, particularly against the matters in paragraphs 1.1. to 1.6;
- the adequacy and quality of Aon's policies in relation to ESG financial considerations, non-financial matters or stewardship and the extent to which Aon has implemented its stated policies;
- how the GAA has considered the Aon Policyholders' interests;
- any concerns raised by the GAA with Aon's governing body and the response received to those concerns;
- how the GAA has sufficient expertise, experience and independence to act in Aon Policyholders' interests;
- the arrangements put in place by Aon, to ensure that the views of Aon Policyholders are directly represented to the GAA; and
- information on the administration charges and transaction costs for each of the Aon Scheme's default arrangement(s), to be published alongside any information relating to the Aon Scheme's default investment strategy and value for members, explaining how an Aon Scheme member can access costs and charges information for each default arrangement and each alternative fund a member can select, including a website link.

2.2 The annual report detailed in 2.1 above shall be sent to the Firm for review and comment before it is finalised. If the Firm wish to change the comments, they will provide additional relevant evidence to justify the changes. The GAA will be obliged to review the comments, but shall not be obliged to amend the report in respect to these comments if they believe the evidence is not adequate. The GAA will be obliged to justify why any of the Firm's comments are disregarded.

2.3 If, having raised concerns with the Firm's governing body about the value for money offered to Aon Policyholders, the GAA is not satisfied with the response of Aon's governing body, the GAA Chair may escalate concerns to the FCA if the GAA believes that would be appropriate. The GAA may also alert Aon Policyholders and employers, and make its concerns public.

2.4 The Chair will raise with Aon's governing body any concerns that the GAA has about the information or resources that Aon provides, or arrangements that Aon puts in place to ensure that the views of Aon Policyholders are directly represented to the GAA. If the GAA is not satisfied with Aon's governing body, the Chair may escalate its concerns to the FCA if appropriate, and may make its concerns public.

## B3. Power to Appoint

3.1 The GAA shall have the power to appoint its own advisers, as it deems appropriate in relation to the execution of its functions.

## B4. Amendment

The GAA and the Firm may decide to amend the Terms of Reference at any time provided:

- such change shall not at any time render the Terms of Reference inconsistent with FCA rules relating to GAAs; and
- three months' notice is given to either party unless it is urgent or there has been or will otherwise be a breach of law or regulation.

# Supplier Security Schedule

## A. OVERVIEW

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

For purposes of this Schedule, "**Confidential Data**" "Confidential Information" refers to Aon's and/or an Aon client's Confidential Information (as defined in the Agreement) and includes, but is not limited to Client Data, Personal Information (or other such similar term as may be defined under applicable law and/or the Agreement. Non-public Information, including information about Aon's operations, Employees, Suppliers, Policies and Practices, Intellectual Property, Financial Data, Technical Information and Trade Secrets.

Capitalized terms used but not defined in this Schedule shall have the meanings assigned to them in the Agreement.

## B. GENERAL REQUIREMENTS: DATA PRIVACY AND SECURITY

1. Data Privacy and Security Programs. Supplier'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 Confidential Data in the possession of Supplier.

2. Data Privacy and Security Policies. Supplier's shall maintain policies and standards for the protection of Confidential Data that originate from industry frameworks and establish uniform security and privacy standards for Supplier's operations. Such policies shall be consistent with ISO27001/2 or another generally accepted industry standard that is applicable to Supplier's 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. Supplier shall abide by these policies, which shall outline the physical, technical, organizational and administrative measures by which Supplier protects Confidential Data. Upon Aon's request, Supplier's shall provide to Aon current copies of such policies.

3. Third Party Subcontractors. Supplier shall be responsible for ensuring that its subcontractors who have Confidential Data maintain data security and privacy programs which are at least as stringent as Supplier's 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. Supplier 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 Supplier:

    a. *Background Checks*. Each individual assigned to perform Services under the Agreement will have been subjected to a background check in accordance with Supplier's background checking policies, which at a minimum includes a criminal history search for the maximum number of years in accordance with state law. 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. Aon reserves the right to request a full background check in compliance with Aon's minimum background check standards.

b. *Training*. Supplier has implemented and maintains a Data Privacy and Information Security awareness program. Upon joining Supplier, employees with access to Confidential Data will be given training on data security and privacy issues as part of their new hire orientation, including on Supplier's current Information Security and Data Privacy Policies. Employees further agree in writing to perform his or her work according to Supplier '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**

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

**1.** Physical Security. Supplier maintains appropriate security controls for entry points, holding areas, telecommunications areas, and cabling areas that contain information processing systems or media containing Confidential 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 Supplier 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. Supplier maintains a clear desk/clear screen policy;

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

e. Visitors to Supplier 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. Supplier maintains the following network security controls and safeguards designed to prevent unauthorized access to Supplier'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 Supplier-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. Supplier maintains the following security controls and safeguards designed to protect and prevent unauthorized access to Confidential 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 Supplier'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 Supplier:

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 Supplier's computing assets and the data contained within these assets, the following safeguards are in place:

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

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

c. Confidential 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 Supplier's custody must be encrypted, sanitized, destroyed, or purged of Confidential Data to ensure that residual magnetic, optical, electrical, or other representation of data has been deleted, and is not easily recoverable, prior to leaving Supplier's custody; and

g. Confidential Data is compartmentalized or otherwise logically separated from, and in no way commingled with other information of Supplier or its other clients.

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

a. Supplier monitors and logs both access and use of the Supplier's system to access Confidential Data, and (ii) keeps a log of each unsuccessful attempt to access the Supplier's system that handles Confidential Data;

b. Access to Confidential 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 Supplier's ability to enforce the confidentiality, integrity, and availability of Confidential 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.

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

**D.** Business Continuity and Disaster Recovery. Supplier will formally develop, document, implement, maintain, monitor and update (as necessary) a plan of action that will guide Supplier in the return of essential business operations, and eventually to a full business recovery, following a Disaster, or business impacting event, to ensure the ability of Aon and Supplier to fulfill obligations under the Agreement and this Security Schedule.

**1.** The following controls will be in place:

a. Supplier declaration procedures
b. Recovery responsibilities
c. Recovery priorities
d. Recovery / resumption strategies
e. Recovery / resumption action plans
f. Recovery requirements (resources and people/third-party vendors)

2. At a minimum, Recovery Time and Recovery Point Objectives will be provided for the following components/services, being provided to Aon.

| Component/Service | Draft RTO Objective | Draft RPO Objective |
|---|---|---|
| Supplier Services | 10 weeks p.a. | 48 hrs. |

3. Supplier will, at a minimum, review, update for material changes, and test/exercise the BC/DR Plan, annually.
4. Supplier will, at a minimum, provide a summary report of the results of the BC/DR Plan, annually.

**E.** Right to Audit. Upon Aon's written request, to confirm compliance with this Agreement and this Security Schedule, as well as any Applicable Laws and industry standards, Supplier shall promptly and accurately complete a written information security questionnaire provided by Aon or a third party on Aon's behalf regarding Supplier's business practices and information technology environment in relation to all Confidential Information being handled and/or services being provided by Supplier to Aon pursuant to this Agreement. Supplier shall fully cooperate with such inquiries.

**F.** Data Breach and Incident Response.

1. **Data Breach**" is defined as any actual or reasonably suspected
   a. unauthorized access to, acquisition of, or use of Confidential Information,
   b. unauthorized or accidental loss, alteration, disclosure, or destruction of Confidential Information;
   c. compromise of the security, confidentiality or integrity of Confidential Information, including but not limited to, a compromise of any physical, technical, administrative or organizational safeguards that relate to the protection of such Confidential Information,
   d. receipt of a complaint alleging unauthorized access to, acquisition of, or use of Confidential Information, or
   e. any incident or event that triggers or implicates Applicable Laws requiring data breach notification to individuals, organizations, or governmental entities.
2. An **"Incident"** is defined as any occurrence that interrupts normal procedure or functioning that is likely to cause harm or inconvenience to the agreed availability of service.

**G.** Notifications. Upon discovery of any actual or reasonably suspected Data Breach, Supplier will immediately notify Aon of such Data Breach and complete Aon's incident response form. Supplier will take immediate and appropriate measures to prevent a recurrence of the Data Breach and will promptly provide reasonable information regarding its remediation efforts.

1. Incident Management Supplier will develop and implement an incident management program, where management and containment of a Data Breach are included as part of the overall mitigation. To the extent any Data Breach is attributable to Supplier (including, if applicable, Supplier's Subcontractors), in whole or in part, Supplier shall bear the costs of: Providing notice to affected individuals as required by Applicable Laws, Providing affected individuals with credit monitoring and identity theft protection (as applicable),Reasonable call center support, if warranted, for such affected individuals for a reasonable period no less than 60 days following the date on which notice of such Data Breach is reasonably expected to be delivered to the affected individuals.

2. Following the occurrence of a Data Breach, Supplier will permit Aon to perform a logical security assessment of Supplier's systems, data processing and business facilities to assess the impact of the event or breach. Supplier will reasonably cooperate with Aon in litigation related to a Data Breach.
3. Supplier shall notify Aon promptly in the event that Supplier is required by law, court order, warrant, subpoena, or other legal or judicial process to disclose any Personal Information to any person other than Aon, or Authorized Persons expressly approved to receive such information by Supplier (unless Supplier is legally prohibited from making the disclosure).
4. Breaches of Confidential Information are subject to unlimited liability

**H.** Privacy and Security Regulatory Compliance

**1.** Compliance with Data Privacy Laws and Regulations. Supplier will comply with data privacy laws and regulations applicable to Supplier 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, Supplier and Aon 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**. PCI. To the extent that Supplier collects, stores, transfers or processes payment card information, Supplier 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.