IHS Markit Standard Terms and Conditions

Securities Finance

1. Definitions and Interpretation

1.1 The following definitions shall apply in this Agreement:

"**Affiliate**" means, in relation to an entity, any company in which such entity (or its ultimate holding company) holds or controls a majority of the issued share capital or such ultimate holding company;

"**Agreement**" means, collectively, the Booking Form and these IHS Markit Terms and Conditions, including the Schedules hereto;

"**IHS Markit Aggregated Data**" means data gathered by IHS Markit from its customers that is commingled in such a way as to prevent anyone identifying the data contributed by individual customers;

"**Booking Form**" means the booking form for securities finance signed by Customer incorporating these IHS Markit Terms and Conditions, including the Schedules, by reference;

"**Business Day**" means a day other than a Saturday or Sunday or a public holiday in London or New York;

"**Commencement Date**" means the date identified as such on the Booking Form;

"**Customer**" means the entity identified as such in the Booking Form;

"**Customer Contact**" means the individual identified by Customer as such on the Booking Form, or subsequently advised from time to time by Customer giving written notice thereof to IHS Markit in accordance herewith;

"**Customer Data**" means Customer's securities lending and borrowing data to be delivered by Customer (or Customer's Data Provider if applicable) to IHS Markit pursuant to this Agreement;

"**Data Delivery Schedule**" means the data delivery schedule attached hereto and identified as Exhibit B;

"**Data Provider**" means, where so agreed, a third party who will provide the Customer Data;

"**Deliverables**" means any document, computer file or other material of whatever nature delivered or to be delivered by IHS Markit in connection with this Agreement, including the Log-ons (as defined below);

"**Fees**" means the fees for the Services payable by Customer as set out on the Booking Form;

"**Indemnifier**" and "**Indemnified**" shall have the meaning given in clause 8;

"**Intellectual Property Rights**" means all:

(a) registered, unregistered, and pending patents, trademarks, service marks, registered designs, applications for any of those rights, trade secrets, trade and business names (including internet domain names and e-mail address names), copyrights, database rights, know-how, and rights in designs and inventions; and

(b) rights of the same or similar effect or nature as or to those in paragraph (a),

in each case in every jurisdiction worldwide;

"**Information Security Terms**" means the Information Security Terms of IHS Markit attached hereto and identified as Exhibit C;

"**Log-on**" means the unique user name and password details provided hereunder to Customer enabling access to those Services available through the Web-site;

"**Outputs**" means such information (in whatever medium) as is provided to Customer by IHS Markit as part of the Service that are provided through the Web-site or made available for Customer to download by secure FTP or through the web-based secure download system known as Sharefile, or through a third-party data service provider, if any, as the case may be;

"**Permissioned Business Unit**" has the meaning ascribed on the Booking Form;

"**Permitted Purpose**" has the meaning ascribed on the Booking Form;

"**Services**" means such services of those described in the Services Schedule as are to be received by Customer from IHS Markit pursuant hereto, being those expressly listed on the Booking Form;

"**Services Schedule**" means the Services Schedule attached hereto and identified as Exhibit A; and

"**Web-site**" means the web site through which those Services that are web-based are to be provided by IHS Markit, and which are accessible through the URL www.ihsmarkit.com/MSF by using the appropriate Log-on.

1.2 In this Agreement:

(a) where a specific remedy is specified herein, it shall be without prejudice to such further or alternative remedies as may otherwise be available in the circumstances;

(b) the term "including" shall not imply any limitation;

(c) the use of a gender shall include other genders and the use of the singular shall include the plural and vice versa.

2. Obligations of IHS Markit

2.1 IHS Markit shall perform the Services using and exercising reasonable care and skill and in compliance with all applicable laws and regulations.

2.2 IHS Markit shall make reasonable efforts to ensure that all the personnel assigned to the performance of its obligations under this Agreement (including the personnel provided by its sub-contractors (if any)) will have the requisite skill, experience, qualifications and knowledge necessary to carry out the tasks assigned to them and in doing so will adopt reasonable and proper standards of behaviour.

2.3 IHS Markit warrants it is appropriately authorised to provide the Services to Customer and that it has such relevant rights, consents and licenses as may be required to enable it to do so.

2.4   IHS Markit shall use reasonable efforts to ensure that the Web-site shall be in good operating condition.

2.5   IHS Markit shall use reasonable efforts at all times to comply with the Information Security Terms.

3.   Obligations of Customer

3.1   Customer shall:

(a)   Deliver, or cause to be delivered by its Data Provider, Customer Data to IHS Markit in accordance with the Data Delivery Schedule;

(b)   ensure that each Log-on provided to Customer by IHS Markit is kept strictly confidential and not shared with, revealed to or used by any other person than the one to whom it was originally issued and takes full responsibility for the consequences of use of its Log-ons other than in accordance herewith;

(c)   inform IHS Markit, immediately, if a Log-on is to be revoked.

3.2   Customer is responsible for the purchase, installation, operation and maintenance of all software, hardware and telecommunications links which may be used or required for the delivery to IHS Markit of Customer Data, the receipt and analysis of Outputs or other Deliverables and any other matter related to the Services.

3.3   Customer warrants that it has taken all requisite corporate actions and obtained all necessary third party consents and licences to enable Customer to:

(a)   supply the Customer Data to IHS Markit in accordance with this Agreement; and

(b)   view all security identifier code types as are identified by IHS Markit as being included in the Services, including CUSIPs, ISINs and SEDOLs; and

(c)   otherwise to fulfil its obligations under this Agreement.

3.4   Customer undertakes to inform IHS Markit of any breach of Clause 3.1(b) as soon as practicable after it becomes aware of such breach and inform IHS Markit of the remedial actions taken by Customer in such respect.

3.5   Customer must not:

(a)   remove or alter any copyright statement included in the Outputs;

(b)   include the Outputs or any information derived from the Outputs in any reports provided to anyone outside the scope of Customer's licence set out in Clause 4; and

(c)   use any of the Services or any of the Outputs in connection with an offering competitive with the Services or designing, creating, improving, providing, sponsoring, administering, calculating, pricing or otherwise supporting any index or other financial product or service (including any algorithm, model, mapping service, benchmark, index, index constituent selection or index hedging, identifier, instrument, reference data, pricing service, liquidity metric, valuation service, any other analytics or any trading platform or pre- or post-trade servicing platform or to store or create a historical database thereof).

3.6   Whenever accessing the Service from a country other than the United Kingdom or United States of America, Customer is solely responsible for ensuring that it is lawful to access and use the Service, the Web-site and the Outputs in such country.

3.7   Customer shall use reasonable efforts at all times to comply with paragraph 12 of the Information Security Terms (Business Continuity Plan).

4.   Intellectual Property and Licence

4.1   As between IHS Markit and Customer, all Intellectual Property Rights arising from or in any respect related to the Services and/or the Outputs (including the data and the format thereof) and all other Deliverables, and in each case all parts and derivatives thereof, shall be and remain vested in IHS Markit from inception.

4.2   As between IHS Markit and Customer, all Intellectual Property Rights in the IHS Markit' Aggregated Data and all parts and derivatives thereof shall be and remain vested in IHS Markit from the moment of creation.

4.3   As between IHS Markit and Customer, the Intellectual Property Rights in the Customer Data shall be and remain vested in Customer.

4.4   IHS Markit grants Customer a revocable, non-exclusive licence for Customer's Permissioned Business Unit to access the Web-site and to use and copy the Outputs only for the Permitted Purpose in accordance herewith. Customer may not publish Outputs or any information derived from the Outputs in any way other than for the Permitted Purpose. Customer shall not use the Outputs in the press, on the internet or otherwise distribute or disclose the Outputs or any information derived from the Outputs outside its Permissioned Business Unit.

4.5   Customer grants IHS Markit an irrevocable, non-exclusive, royalty-free licence to use the Customer Data to generate the IHS Markit Aggregated Data and to provide the Services.

4.6   The licences granted under this clause 4 may only be extended or modified by written agreement executed by the parties hereto.

5.   Fees and Suspension of Services

5.1   Customer shall pay to IHS Markit the Fees set out in the Booking Form.

5.2   Fees shall be invoiced by IHS Markit annually in advance.

5.3   Invoices are payable within 30 days of the date thereof. Interest shall be due and payable on overdue invoices that are not the subject of a *bona fide* dispute from the due date of the invoice until the date of payment and interest will continue to accrue following a judgment (if any) ordering payment of such invoice. The rate of interest will be 2% per year above the base rate for the time being of HSBC Bank plc, or such higher rate as is required by applicable law.

5.4   The Fees specified herein are exclusive of any applicable taxes, including without limitation value added tax, on sales or supplies in any applicable jurisdiction and Customer must pay these to IHS Markit as well as the amounts concerned where such taxes apply. For the avoidance of doubt, where subsequent to an invoice of the Fees it is determined that a tax on sales or supplies was payable in respect of all or part of the Services but was not included in the relevant invoice, IHS Markit may invoice

Customer for such tax and Customer shall pay such invoice as set forth above.

5.5   IHS Markit shall have the right but not the obligation to suspend providing Services to Customer, or, at its option, may terminate this Agreement, in the event Customer:

(a)   is late in making any payment of an invoice (other than one under a bona fide dispute) by more than 28 days from the due date; and/or

(b)   is not providing Customer Data in accordance with its obligations hereunder.

5.6   IHS Markit may only increase the Fees once in any 12 month period, such increase to be no more than the aggregate of 5% plus:

(a)   in the event Customer is identified on the Booking Form as being based in the United States of America, the US CPI (Consumer Price Index) during the previous 12 month period; or

(b)   in the event Customer is identified on the Booking Form as being based outside the United States of America, the United Kingdom's RPI (Retail Price Index) during the previous 12 month period,:

provided that IHS Markit shall give Customer no less than 3 months notice before applying any such increase. Upon such an increase being effective other than on a renewal hereof, IHS Markit may invoice Customer for the amount of such increase pro rated to the next renewal date.

6.   Use of the Services

If IHS Markit reasonably believes that Customer is permitting use of any Deliverable, Log-on or Output otherwise than in accordance herewith, IHS Markit shall notify Customer, and Customer shall promptly use its best efforts to ensure any such use ceases. IHS Markit may suspend the Services to Customer if such non-compliant use persists, and in any event may immediately block the relevant Log-on.

7.   Confidentiality

7.1 Each party shall keep confidential any information disclosed to it by the other party in connection with this Agreement, whether directly or indirectly and by any means ("Confidential Information"). This includes all information so disclosed comprising or relating to the Outputs, Deliverables, Customer Data, the business affairs, operations and processes of either party or those of its clients or customers and any information that is marked as being confidential or which, from its nature, content or the circumstances in which it is provided, might reasonably be supposed to be confidential. Neither party shall disclose the other's Confidential Information to anyone else except to:

(a)   the disclosee's employees who need such Confidential Information in order to enable the party concerned to carry out any of its obligations under this Agreement or who are expressly permitted to have access to such Confidential Information hereunder;

(b)   the disclosee's auditors or lawyers; or

(c)   any temporary staff, contractors or consultants working for the disclosee with a need to know;

provided that disclosure of the Confidential Information is necessary in order to enable the person to whom it is disclosed to carry out the work

concerned; or otherwise in accordance with this Agreement. Each party shall be responsible for ensuring that any person to whom Confidential Information is disclosed by them complies with obligations of confidentiality substantially similar to those in this clause 7.1.

7.2   The obligations of confidentiality set out in clause 7.1 do not apply to any information that is:

(a)   generally available to the public, unless this availability results from a breach of this Agreement;

(b)   already in the possession of the party receiving the information or which it obtains or originates independently in circumstances in which that party is free to disclose it to others;

(c)   trivial or obvious; or

(d)   required to be disclosed by any court, tribunal or regulatory authority that is entitled by law to order its disclosure, save that in such instance the party whose Confidential Information is so required shall, to the extent permissible by law, be afforded the opportunity to make representations to such body in relation to such disclosure for the purpose of minimising the extent and effect of such disclosure.

8.   Indemnities

8.1   Subject to clause 9 and to compliance by Customer with clause 8.3, IHS Markit shall indemnify Customer against each loss, liability and cost (including reasonable legal costs and attorneys' fees) that Customer incurs or becomes liable for arising out of a claim of infringement of an Intellectual Property Right howsoever arising as a result of or in connection with the use of the Outputs and any other Deliverables or any part of them by the Customer in accordance with this Agreement (including, without limitation, each loss, liability and cost incurred as a result of defending or settling such claim).

8.2   Subject to clause 9 and to compliance by IHS Markit with clause 8.3, Customer shall indemnify IHS Markit against each loss, liability and cost (including reasonable legal costs and attorneys' fees) that IHS Markit incurs or becomes liable for arising out of a claim of (a) infringement of an Intellectual Property Right howsoever arising as a result of or in connection with the receipt or use of the Customer Data or any part of it in accordance with this Agreement (including, without limitation, each loss, liability and cost incurred as a result of defending or settling such claim); or (b) by a third party in connection with any third party's access or use of any of the Services (or any data forming part of the Services) permitted or suffered by Customer or its Affiliates (excluding claims covered under 8.2(a)).

8.3   If a party ("**Indemnified**") becomes aware of a matter which might give rise to a claim against it as contemplated under clause 8.1 or 8.2:

(a)   the Indemnified shall promptly notify the other party ("**Indemnifier**") of the matter and consult with the Indemnifier with respect to the matter; provided, any failure by the Indemnified to provide such notice will not relieve the Indemnifier of its indemnification obligations under this Agreement except to the extent the Indemnifier can demonstrate actual, material prejudice to its ability to mount a defence as a result of such failure.

(b)   the Indemnified shall provide to the Indemnifier and its advisors reasonable access to premises and personnel and to all relevant assets, documents and records that it possesses or controls as may be necessary or expedient in order for the Indemnifier to properly deal with such claim;

(c)   the Indemnified shall:

  (i)   take any action and institute any proceedings, and give any information and assistance the Indemnifier may reasonably request to dispute, resist, appeal, compromise, defend, remedy or mitigate the matter, or enforce against a person (other than the Indemnified) Indemnifier's rights in relation to the matter; and

  (ii)   if the Indemnifier so requests, allow the Indemnifier the exclusive conduct of the proceedings,

in each case provided that the Indemnifier shall indemnify the Indemnified for all reasonable costs incurred as a result of such request or choice, and the Indemnified may retain its own counsel at the reasonable cost of the Indemnifier in the event of a bona fide conflict of interest in relation to the indemnified matter where the Indemnifier assumes exclusive conduct of the proceedings as aforesaid.

(d)   The Indemnified shall not admit liability in respect of or settle the matter nor otherwise knowingly prejudice the defence of the claim without first obtaining the Indemnifier's written consent (not to be unreasonably withheld or delayed).

8.4   Notwithstanding the indemnities in this clause 8, the Indemnified shall be obliged to mitigate such losses as it may incur in respect of such indemnified matters.

9.   Exclusions and limitations

9.1   Neither party's liability is excluded or limited by any provision of this Agreement for:

  (a)   death or personal injury caused by the party's negligence or the negligence of the party's employees or agents;

  (b)   breach of the limitations on use of the Outputs

  (c)   fraudulent misrepresentation; or

  (d)   an obligation to pay sums properly due and owing to the other in the course of normal performance of this Agreement.

9.2   Subject to clause 9.1, neither party shall be liable to the other under or in relation to this Agreement or the Services (whether such liability arises due to negligence, breach of contract, misrepresentation or for any other reason) for any loss of or damage to: profits, sales, turnover, contracts, customers, business, reputation, software, data, wasted management or other staff time, losses or liabilities under any other contracts or any indirect, special or consequential loss or damage: regardless of whether the relevant party was aware of the possibility of such matter. The term "loss" as used herein includes a partial loss or reduction in value as well as a complete or total loss.

9.3   Subject to clauses 9.1 and 9.2, each party's total liability arising from or in connection with this Agreement (and whether the liability arises because of breach of contract, negligence, misrepresentation or for any other reason) shall be limited to the annual Fees payable by

Customer in respect of the year in which the relevant liability arises.

9.4   Customer recognises that the Outputs (and any other Deliverables) are performance analysis tools designed to assist in the making of investment decisions and the management of securities portfolios, but that Customer shall have and bear sole and complete responsibility for all such decisions and management. Accordingly, IHS Markit will not be liable under this Agreement (even where any other term of this Agreement might suggest otherwise) or in tort (including negligence) or otherwise for any losses, damages, expenses, legal actions or claims whatsoever incurred or sustained by Customer relating to the quality or appropriateness of any analysis, recommendations, advice or decisions made (in whole or in part) with the aid of any Output (or other Deliverable).
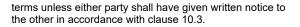
9.5   Each party (a) acknowledges that, in entering into this Agreement, it has not relied on any representation or warranty made by the other party that has not been set out in this Agreement; (b) agrees that it will not rely on any representation or warranty made by the other party except to the extent that the representation or warranty concerned is contained in this Agreement; and (c) no conditions, warranties or other terms apply to any Services or Deliverables supplied under this Agreement except to the extent that they are expressly set out in this Agreement. No implied conditions, warranties or other terms shall apply (including any implied terms as to satisfactory quality, fitness for purpose or conformance with description).

9.6   IHS Markit DOES NOT GUARANTEE THE ACCURACY AND/OR THE COMPLETENESS OF ANY DELIVERABLE SUPPLIED BY IT OR ANY INFORMATION INCLUDED THEREIN. IHS Markit MAKES NO WARRANTY, EXPRESS OR IMPLIED, AND EXPRESSLY DISCLAIMS ALL WARRANTIES AS TO RESULTS TO BE OBTAINED BY CUSTOMER OR ANY OTHER PERSON OR ENTITY FROM THE USE OF THE DELIVERABLES SUPPLIED BY IHS Markit OR ANY INFORMATION INCLUDED THEREIN. IHS Markit MAKES NO EXPRESS OR IMPLIED WARRANTIES, AND EXPRESSLY DISCLAIMS ALL WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE WITH RESPECT TO THE DELIVERABLES SUPPLIED BY IHS Markit OR ANY INFORMATION INCLUDED THEREIN. WITHOUT LIMITING ANY OF THE FOREGOING, IN NO EVENT SHALL IHS Markit HAVE ANY LIABILITY FOR ANY SPECIAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS), EVEN IF NOTIFIED OF THE POSSIBILITY OF SUCH DAMAGES.

9.7   Where the Outputs are identified in the Booking Form as being provided through a third party's data service or otherwise provided through a third party service, IHS Markit shall have no liability or responsibility to Customer for the quality, functionality or any other aspect of such service, or the accuracy, timeliness or completeness of Outputs received by Customer through such service, and Customer shall be solely responsible for maintaining a services agreement directly with the provider of such service for usage of Outputs. Customer agrees not to make any claim against such third party service provider in relation to any aspect of the Outputs, including quality, fitness for purpose or conformance with description thereof.

10.   Termination

10.1   This Agreement shall be binding upon signature of the Booking Form. The term of this Agreement shall commence on the Commencement Date and shall continue until terminated pursuant to this clause 10. This Agreement will renew automatically for successive 12 month renewal

terms unless either party shall have given written notice to the other in accordance with clause 10.3.

10.2   Without prejudice to any rights that have accrued under this Agreement, either party may terminate this Agreement immediately in the event that:

(a)   the other breaches a material obligation or warranty under this Agreement and, in the case of a breach capable of remedy, the other has failed to remedy such breach within 20 Business Days of a notice requiring such remedy; or

(b)   the other party suspends, or threatens to suspend, payment of its debts or is unable to pay its debts as they fall due or admits inability to pay its debts or is deemed unable to pay its debts as they fall due pursuant to relevant applicable insolvency laws; or

(c)   the other party commences negotiations with all or any
class of its creditors with a view to rescheduling any of its debts, or makes a proposal for or enters into any compromise or arrangement with its creditors or an arrangement pursuant to any bankruptcy act or insolvency laws, other than for the sole purpose of a scheme for a solvent amalgamation of that other party with one or more other companies or the solvent reconstruction of that other party; or

(d)   the other party is adjudicated as bankrupt or a petition in bankruptcy is filed by or against the other party;

(e)   a petition is filed, a notice is given, a resolution is passed, or an order is made, for or in connection with the winding up of that other party other than for the sole purpose of a scheme for a solvent amalgamation of that other party with one or more other companies or the solvent reconstruction of that other party; or

(f)   an application is made to court, or an order is made, for the appointment of an administrator or if a notice of intention to appoint an administrator is given or if an administrator is appointed over the other party; or

(g)   a floating charge holder over the assets of that other party has become entitled to appoint or has appointed an administrative receiver; or

(h)   any event occurs, or proceeding is taken, with respect to the other party in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned in clause 10.2(b) to (g) inclusive.

10.3   Either party may elect for this Agreement not to renew at the end of the then current term hereof by giving the other not less than 90 days' prior written notice.

11.   Consequences of termination

11.1   On termination of this Agreement by Customer in accordance with clause 10.2, IHS Markit will remit to Customer a pro rata amount of any Fees received in respect of the relevant unexpired period to the end of the then current term hereof.

11.2   Termination shall not affect the accrued rights and liabilities of the parties.

11.3   The provisions of clauses 1 (definitions and interpretation), 4.1, 4.2, 4.3, 4.5 and 4.6 (intellectual property and licence), 6 (use of data), 7 (confidentiality), 8 (indemnity), 9 (exclusions and limitations), 11 (consequences of termination) and 14 (general) shall survive any expiry or termination of this Agreement and shall remain in full force and effect.

12.   Data Protection

12.1   Customer acknowledges that, pursuant to the Agreement, IHS Markit may receive information from Customer about some or all of Customer's individuals. This information may include personal data such as names, company names, titles, work contact information, personal contact information, and payment information ("Personal Data").

12.2   IHS Markit will handle all Personal Data in accordance with

IHS Markit's Privacy and Cookie Policy which can be found at 12.3 http://www.markit.com/General/Privacy-and-Cookie-Policy. In

order to provide the Services and Outputs IHS Markit may:

(a)   Use, collect, store, disclose and process the Personal Data; and

(b)   Transfer the Personal Data inside of, and outside of, the European Economic Area.

12.4   Customer represents that those individuals for which they provide Personal Data to IHS Markit, have consented to the processing and transfer of their Personal Data as set out in this Section 12.

13.   Trial/Evaluation

13.1   Upon Customer's written request, IHS Markit may grant Customer access to certain securities finance data services ("Trial Services") as determined by IHS Markit in its sole discretion, in order to permit Customer to evaluate such Trial Services

13.2   Subject to the terms and conditions of clause 13.1 through 13.4, IHS Markit grants to Customer a non-exclusive, limited, personal, non-transferable, terminable license to internally evaluate the Trial Services for a period not to exceed thirty (30) days from making such Trial Services available to Customer ("Trial Period"). Access to the Trial Services will be for a maximum of five (5) individual identified users, unless otherwise agreed in writing.

13.3   CUSTOMER AGREES THAT THE TRIAL SERVICES PROVIDED OR MADE AVAILABLE TO CUSTOMER PURSUANT TO SECTIONS 13.1 THROUGH 13.4 ARE PROVIDED ON AN "AS IS" BASIS AND THAT, TO THE MAXIMUM EXTENT ALLOWED BY LAW, NEITHER IHS MARKIT NOR ITS AFFILIATES NOR ANY THIRD PARTY MAKE(S) ANY REPRESENTATION, WARRANTY, CONDITION, UNDERTAKING OR TERM, WHETHER EXPRESS, IMPLIED OR STATUTORY, REGARDING OR RELATING TO THE TRIAL SERVICES, INCLUDING: (A) OF MERCHANTABILITY, NONINFRINGEMENT OR FITNESS FOR ANY PARTICULAR PURPOSE; OR (B) AS TO THE CONTINUITY, ACCURACY, TIMELINESS OR COMPLETENESS OF ALL OR ANY PART THEREOF; OR (C) AS TO ANY RESULTS TO BE ATTAINED BY CUSTOMER OR INDIVIDIUAL IDENTIFIED USERS FROM THE USE OF ALL OR ANY PART THEREOF.

13.4   Upon expiry of the Trial Period the Customer shall, cease using the Trial Services and within thirty (30) days

thereof purge or delete the Trial Services from its electronic or other systems unless subscribing to the Services under a valid contract. Customer shall reasonably cooperate with Markit in connection with any request to verify its compliance with this clause 13.4.

14.   General

14.1   No amendment to this Agreement shall be effective unless in writing and signed on behalf of both parties. However, and notwithstanding the preceding, IHS Markit may update these IHS Markit Standard Terms, including by way of example the descriptions of Services in the Services Schedule and the contents of the Data Delivery Schedule and Information Security Terms, from time to time by amending such Schedule, uploading the amended IHS Markit Standard Terms to the relevant website and notifying Customer no less than 30 days prior to any material amendment taking effect, provided that no such amendment shall have the effect of being materially more onerous or less beneficial to Customer in any case unless mutually agreed in writing between the parties.

14.2   Any inconsistencies between the documents comprising this Agreement shall be resolved in the following order of priority:

(a)   the Booking Form;

(b)   these IHS Markit Terms and Conditions;

(c)   the Services Schedule;

(d)   the Data Delivery Schedule; and finally

(e)   the Information Security Terms.

14.3   All notices, agreements and consents under this Agreement shall be in writing. Notices shall be deemed effectively served if sent to the address of the relevant party set out on the Booking Form or to such other address as either party shall notify to the other in accordance with this clause 13.3, provided that no notice to IHS Markit shall be effective unless a copy has been sent to the attention of IHS Markit's Legal Team at IHS Markit's address as specified on the Booking Form. Any such letter may be delivered by hand or first class pre-paid letter and shall be treated as having been delivered(a) if delivered by hand, when so delivered; or (b) if by first class post, 5 days after posting.

14.4   Notwithstanding any other provision of this Agreement, neither party will be responsible or liable for any delay or failure in performing any of its obligations under this Agreement if such delay or failure is caused by circumstances outside its reasonable control and unknown to it at the date of this Agreement, including any failure or delay in the operation of any third party network, hardware, software or telecommunications link.

14.5   If a party (a) delays in enforcing its rights under this Agreement (whether in relation to a breach by the other party or otherwise); or (b) agrees not to enforce its rights, or

to delay doing so, then unless such party expressly agrees otherwise, that delay or agreement shall not be treated as waiving the rights of such party. Any waiver of a party's rights in relation to a particular breach of this Agreement shall not operate as a waiver of any subsequent breach. No right, power or remedy to which either party is entitled under this Agreement is exclusive of any other right, power or remedy available to that party.

14.6   This Agreement is personal to the parties and neither party may assign its rights or obligations under it without the consent of the other party provided that IHS Markit may

(a)   assign its rights under this Agreement to an Affiliate of
IHS Markit by notifying Customer; or

(b)   subcontract its obligations hereunder to any of its Affiliates:

provided that in each case IHS Markit shall remain ultimately responsible to Customer for IHS Markit's obligations hereunder. Further, IHS Markit may assign its rights under this Agreement in connection with the sale of all or substantially all of the shares or assets of IHS Markit or its holding company.

14.7   A person who is not party to this Agreement may not enforce any of its terms.

14.8   If any provision of this Agreement is held for any reason to be ineffective or unenforceable, this shall not affect the validity or enforceability of (a) any other provision of this Agreement; or (b) the agreement as a whole.

14.9   This Agreement is the parties' entire agreement with respect to its subject matter and supersedes any prior agreement or oral or written representations with respect thereto.

14.10   In the event that Customer is identified on the Booking Form as being based in the United States of America, this Agreement shall be governed by the laws of the State of New York; otherwise this Agreement shall be governed by the laws of England and Wales, in each case without regard to any conflicts of laws principles. This agreement shall be subject to arbitration by a single arbitrator under the international arbitration rules of the American Arbitration Association, with the location of such arbitration to be in the location of the usual place of business (or in the case of multiple such locations, the place of incorporation) of the other party to the one bringing the relevant action. The arbitrator in such circumstance shall be empowered to award attorneys' fees to the prevailing party in any such arbitration. However, notwithstanding anything to the contrary herein, either party may bring an action for an injunction, specific performance or other non-monetary relief in the courts of the relevant jurisdiction, which shall be the courts of the state or country determined in accordance with this clause 14.10.

EXHIBIT A

SERVICES SCHEDULE

This Services Schedule ("**Services Schedule**") constitutes a description of all IHS Markit's various available services. The Services that Customer is entitled to receive shall be those listed in the Booking Form, subject to the terms of this Agreement. In this Services Schedule, terms not otherwise defined have the meaning given elsewhere in this Agreement.

1.   Performance Explorer Service

1.1   The PX Service is a securities lending and borrowing performance analysis service provided by means of a website ("**PX Website**") that Customer may log on to through the website found at www.ihsmarkit.com/MSF, using Log-ons issued by IHS Markit for such purpose.

1.2   The PX Service enables organisations involved in securities lending to compare their performance against a non-identifiable aggregated group. Inventory (in the case of lenders) and positions information is received from subscribers to relevant services from IHS Markit ("Group Members"), giving a snapshot of their data at the close of business on each Business Day, in each case in accordance with the Data Delivery Schedule (or contractual provisions substantially similar thereto). The PX Service data is published on the relevant subsequent Business Day (in relation to the date of data submission) as set out in the Data Delivery Schedule.

1.3   Each client sees their own data plus anonymised and aggregated group data to transaction level. Filtering enables either "like for like" comparison or the opportunity to compare against those employing different strategies. There are also tools for "what if" scenarios and ranking performance against an internal or external peer group.

1.4   The PX Service includes the following:

(a)   processing of Customer Data submitted by Customer and of data supplied by other subscribers to the PX Service to produce Group Outputs and Customer Outputs as noted below;

(b)   use of the PX Website to explore the Customer Outputs and the Group Outputs, which are made available in accordance with the timescale set out in the Data Submission Schedule;

(c)   such training of Customer's Permissioned Business Unit in the use of the PX Website as may be necessary or desirable to fully understand and benefit from the PX Service, the scheduling and location of which to be agreed between IHS Markit and Customer.

1.5   The PX Website has two types of output: Group Outputs and Customer Outputs:

(a)   the Group Outputs show information based on the IHS Markit Aggregated Data, which pertains to all Group Members including Customer, and will be based on the Customer Data supplied by Customer and the data supplied by the other Group Members; and

(b)   the Customer Outputs will show data pertaining to Customer and will be based solely on the Customer Data supplied by Customer.

1.6   The Group Outputs are supplied to all Group Members who have subscribed to the PX Service, whereas Customer Outputs are only available to Customer. Customer's data is safeguarded by IHS Markit in accordance with the terms of this Agreement. Therefore Customer will be able to review its own performance in relation to other Group Members but will not be able to identify the performance of any other Group Member and vice versa.

1.7   Where Customer has subscribed for the PX Service and is submitting Customer Data in respect of its securities lending clients on behalf of whom Customer lends securities as an agent or principal ("**Underlying Clients**"), Customer will be eligible to subscribe for Internal Underlying Client Access and/or External Underlying Client Access.

1.8   Eligibility to subscribe for the PX Service is not contingent upon subscription to any other service from IHS Markit.

2.   Transaction Explorer Service

2.1   Transaction Explorer ("**TX Service**") is an additional tool available as an add-on to the PX Service, which is provided via outputs available on the PX Website. The TX Service gives Customer access to "pre trade" and "at trade" information based on the IHS Markit's Aggregated Data.

2.2   Eligibility to subscribe for the TX Service is not contingent upon Customer's subscription to any other service.

3.   Internal Underlying Client Access

3.1   Internal Underlying Client Access is functionality within the PX Service that allows Customer to view, within the PX Service, Customer Outputs that are specific to the submitted Customer Data in respect of a particular Underlying Client.

3.2   Internal Underlying Client Access shall only be available to Customer in relation to relevant Underlying Clients where this has been noted in the Booking Form or subsequently agreed between the Customer and IHS Markit in writing.

3.3 Eligibility to subscribe for Internal Underlying Client Access is contingent upon Customer's subscription to the PX Service.

4. External Underlying Client Access

4.1 Where Customer has subscribed for External Underlying Client Access for a particular Underlying Client, IHS Markit will provide that Underlying Client with log-ons that permission such Underlying Client to access the PX Website and see certain simplified Customer Outputs in respect of such Underlying Client's own Customer Data (as submitted by Customer) to granularity level 6, which is equivalent to named equity indices, e.g. S&P500, subject to the Agreement. These simplified Customer Outputs **exclude** the following functionality:

      (a) individual security and transaction levels that underlay such Outputs;

      (b) the setting of targets for performance; and

      (c) the production of time-series graphs and instrument-level (e.g. ISIN-level) search capability.

4.2 Where Customer has subscribed to External Underlying Client Access for an Underlying Client, Customer may, at Customer's option, elect to have such Underlying Client receive Customer Outputs in respect of such Underlying Client's data that are not simplified as aforesaid, but rather with full available granularity in respect of such Customer Outputs.

4.3 External Underlying Client Access shall only be available to Customer in relation to relevant Underlying Clients where this has been noted in the Booking Form or subsequently agreed between the Customer and IHS Markit in writing and signed by both parties.

4.4 Customer shall remain responsible to IHS Markit for compliance by its Underlying Clients who have been granted External Underlying Client Access with the requirements of the terms of this Agreement as they pertain to recipients of the PX Service.

4.5 Eligibility to subscribe for External Underlying Client Access for Underlying Clients is contingent upon Customer's subscription to the PX Service.

5. International Index Explorer Service

5.1 The International Index Explorer service ("**IIX Service**") allows subscribers to access data pertaining to securities financing in relation to a security, which constitutes an indicator for the level of short selling in that security.

5.2 The IIX Service is provided through a secure website ("**IIX Website**") that Customer may log on to through the website found at www.ihsmarkit..com/MSF, using Log-ons issued by IHS Markit for such purpose.

5.3 The IIX Service enables typical users (which include portfolio managers, analysts, members of dealing teams and securities financing traders) to better understand securities lending and borrowing flows within the relevant financial markets.

5.4 The available data in the IIX Service spans global fixed income and equity asset classes, indices and sectors; however, the IIX Service data that Customer will have access to will depend upon the scope of access for which Customer has subscribed, as noted in the Booking Form. Global access constitutes access to all available data through the IIX Service.

5.5 Customer is able to search for the relevant security using the search functionality in the IIX Website and if that security is available within Customer's subscription, Customer will be presented with a number of graphs and tables generated by the IIX Service relating to that security, showing details of securities financing information in relation to that security. Information is available in graphical, tabular and heat-map form.

5.6 The data in the IIX Service is based on the wholesale IHS Markit's Aggregated Data, which is updated on a daily basis on a rolling delay of one Business Day.

5.7 Eligibility to subscribe for the IIX Service is not contingent upon subscription to any other service from IHS Markit.

6. Data Downloads Service

6.1 The Data Downloads Service comprises extracts from IHS Markit's Aggregated Data. The Data Downloads Service includes data across specific classes of fixed income and/or equity instruments as available in the type of download listed in the Booking Form, subject to amendment by written agreement between IHS Markit and Customer from time to time.

6.2 The Data Downloads are files provided by IHS Markit to Customer via secure file transfer protocol (known as SFTP) or such other appropriately secure method as IHS Markit may determine from time to time, on Business Days during the term of the Agreement. The fields of data included in the daily Data Downloads will be those available in the type of download as is specified in the Booking Form.

6.3 Eligibility to subscribe for the Data Downloads Service is not contingent upon subscription to any other service from IHS Markit.

7. Risk Explorer Service

7.1   The Risk Explorer service ("**RX Service**") enables subscribing Customers to more fully understand the risks presented by their securities lending portfolios, based on their Customer Data submitted to IHS Markit.

7.2   The RX Service is provided through either:

(a)   a secure website ("**RX Website**") that Customer may log on to through the website found at www.https://ihsmarkit.com/login.html, using Log-ons issued by IHS Markit for such purpose; or

(b)   a series of reports to be provided by IHS Markit to Customer in .PDF format or hard copy, at Customer's option ("**RX Reports**") as specified on the Booking Form.

7.3   This Risk Explorer service involves:

(a)   processing of the Customer Data using the Risk Explorer methodology set out in the document entitled "Risk Methodology" provided to Customer and subject to such updates as may be advised to Customer from time to time, including measurement of both securities lending and cash collateral reinvestment risks; and

(b)   delivery of the product of such processing ("**RX Outputs**") to Customer through the RX Website for Customer to review and explore.

7.4   Using the Customer Data supplied, IHS Markit calculates the value at risk, expected loss on default and risk premium, which are used to calculate additional RX Outputs.

7.5   The frequency that the Customer receives the RX Outputs will be as specified in the Booking Form.

7.6   Eligibility to subscribe for the RX Service is not contingent upon subscription to any other service from IHS Markit.

8.   External RX Access

8.1   Where Customer has subscribed for External RX Access for a particular Underlying Client, IHS Markit will provide that Underlying Client with the RX Service in respect of such Underlying Client's Customer Data as provided by Customer.

8.2   External RX Access shall only be available to Customer in relation to relevant Underlying Clients where this has been noted in the Booking Form or subsequently agreed between the Customer and IHS Markit in writing.

8.3   Customer shall remain responsible to IHS Markit for compliance by its Underlying Clients who have been granted External RX Access with the requirements of the terms of this Agreement as they pertain to recipients of the RX Service.

8.4   Eligibility to subscribe for External RX Access for Underlying Clients is contingent upon Customer's subscription to the RX Service.

9.   IHS Markit Toolkit

9.1   The IHS Markit Toolkit for Microsoft Excel ("**DX Toolkit**") is a downloadable add-in to Microsoft Excel, providing functionality to appropriately permissioned individual identified users within Customer so as to enable those users to import certain data and information directly into a Microsoft Excel spreadsheet and manipulate such data using Microsoft Excel. The data and information available to such users through the DX Toolkit ("**DX Toolkit Data**") will be as set out in the Booking Form. If Customer's Booking Form uses the former terminology "Investment Management Toolkit" or "IM Toolkit" (which are subsets of the DX Toolkit) then such information and data available through the DX Toolkit shall be that which is available to Customer through their subscription to the IIX Service.

9.2   Use of the DX Toolkit requires the relevant appropriately authorised personnel hereunder to download and install an add-in to Microsoft Excel, and in the process to agree on behalf of Customer the terms applying to the DX Toolkit that are provided and displayed at the time of such installation with the installation instructions on the Web-Site. No personnel without a Log-on shall be entitled to access the web page that enables installation of the DX Toolkit.

9.3   No DX Toolkit Data or any derivative thereof shall be made available or otherwise distributed to any personnel other than an individual identified user of the DX Toolkit hereunder.

9.4   Customer may elect to have additional users of the DX Toolkit beyond those users included in the DX Toolkit base licence by notifying IHS Markit in writing and paying such additional Fees as are specified in the Booking Form (or if not so specified, such additional Fees as are customarily charged by IHS Markit for additional users at the relevant time) which shall be payable in advance and invoiced on a pro rata basis in accordance with this Agreement to the next renewal date and thereafter invoiced together with the other Fees hereunder. Any such written notification of additional users of the DX Toolkit shall not be capable of being withdrawn or cancelled, provided that Customer may reduce the number of such additional users at the next renewal hereof by giving not less than 90 days prior notice.

9.5   Eligibility to subscribe for the DX Toolkit requires the relevant user to have a copy of and a valid licence to use Microsoft Excel software.

10.   Reporting Packages

10.1   IHS Markit's risk management reports ("**Risk Management Reports**") are reports that are provided weekly, monthly, quarterly or annually as specified in the Booking Form and are available for beneficial owners who lend securities. Risk Management Reports provide text, graphic and numeric detail information in PDF format showing the potential magnitude of any losses and the likelihood of such losses occurring in relation to the recipient's lending programme. Risk Management Reports also show, where Customer also invests cash collateral, the likely daily variability in mark to market values and how this variability is driven by yield curve movements, credit spreads and currency movements, and includes assessment of likely loss in the event of an issuer of a money market instrument defaulting.

10.2   IHS Markit's performance review reports ("**Performance Review Reports**") are reports that are provided weekly, monthly, quarterly or annually as specified in the Booking Form and are available for beneficial owners who lend securities. Performance Review Reports provide text, graphic and numeric detail information in PDF format showing the performance, strengths and weaknesses in Customer's lending programme, assessed against Customer's peer group.

10.3   IHS Markit's board reports ("**Board Reports**") are reports that are provided weekly, monthly, quarterly or annually as specified in the Booking Form and are available for beneficial owners who lend securities. Board Reports provide a high-level oversight snapshot of Customer's securities lending programme, suitable for updating Trustee Boards or Senior Management.

10.4   Eligibility to subscribe for Risk Management Reports, Performance Reports or Board Reports is not contingent upon subscription to any other services.

11.   Third Party Market Data Platforms

11.1   The Booking Form may identify a third party platform provider as being the delivery mechanism for the Outputs that are to be received hereunder, being extracts from the IHS Markit's Aggregated Data as identified in the Booking form, in which case IHS Markit shall arrange for enablement of Customer's relevant Permissioned Business Unit to access such Outputs through such platform.

11.2   If for any reason the Outputs become unavailable through such platform on an ongoing basis, IHS Markit shall make available to Customer an alternative method of receiving the relevant Outputs.

11.3   Eligibility to subscribe for the Outputs through a third party platform provider is not contingent upon subscription to any other services from IHS Markit, but does require Customer to maintain a services agreement with the relevant third party platform provider for continued access to such platform.

EXHIBIT B

DATA DELIVERY SCHEDULE

In order to receive Services from IHS Markit, Customer must provide its Customer Data on each Business Day in accordance with this Data Delivery Schedule.

1.   Data to be provided

1.1   IHS Markit must receive data pertaining to Customer's securities lending and borrowing, including inventory and lent assets and details of all securities lending and borrowing transactions ("**Customer Data**") in accordance with the applicable Data Interface Specifications set out in the relevant Appendix or Appendices hereto, as identified on the Booking Form. The Data Interface Specifications shall be subject to such updates as IHS Markit may notify Customer from time to time, save that any such updates shall not cause the applicable Data Interface Specifications applying to Customer to be materially more onerous on Customer than those in place immediately prior to such update.

1.2   Unless otherwise expressly stated, the Customer Data provided hereunder is to relate to Customer's Permissioned Business Unit and, if applicable, Customer's Underlying Clients.

1.3   Customer must either provide its Customer Data to IHS Markit directly or must otherwise arrange for its Data Provider (if applicable) to do so. Where Customer's data is provided by a Data Provider, this shall be noted on the Booking Form, and all references to Customer's obligations in relation to Customer Data in this Data Delivery Schedule shall be interpreted as a requirement for Customer to procure that its Data Provider complies with such obligation.

1.4   Customer Data shall accurately reflect the business that is being conducted and must not be manipulated in any way to deliberately impact apparent performance.

1.5   Where applicable, Customer may also contribute additional data types and other such data types as the parties may in future agree ("**Further Data**") as defined in the Contributed Data Specification section of the IHS Markit Services Agreement Booking Form. This may include, but is not limited to:

(a)   Collateral, cash and non cash transactions

(b)   Intraday transactions

(c)   Pending transactions

(d)   Exclusive transactions

1.6   Markit shall make Further Data available only to its clients using equivalent services who are providing their equivalent data (for example, for Pending transaction data, Markit shall only make available to clients who are providing their equivalent Pending data)

2.   Process and timescale for delivery of Customer Data

2.1   The frequency of provision of Customer Data will depend upon the frequency of the most frequent Services to be received pursuant to the Booking Form. However, unless expressly agreed otherwise on the Booking Form, Customer must provide Customer Data daily on Business Days.

2.2   Where Customer Data is provided daily on Business Days, Customer shall submit Customer Data in accordance with the following deadlines, based on the location from which the Customer Data is provided, where "T" is the date to which the relevant Customer Data relates:

(a)   Customer Data from Asia Including Australasia: by 11:00 am GMT on T;

(b)   Customer Data from Europe: by 11:59 pm GMT on T; and

(c)   Customer Data from North America: by 02:00 am GMT on T.

3.   Exclusions to Customer Data

3.1   Following receipt of Customer Data, IHS Markit shall prepare summary figures and apply a threshold analysis using such thresholds as may have been agreed between Customer and IHS Markit or in the absence of such agreement, as appear appropriate to IHS Markit in the circumstances, in each case designed to identify errors and anomalies. Customer Data that breaches such thresholds shall be identified as exclusions ("**Exclusions**"). IHS Markit shall provide such summary figures and Exclusions to Customer as soon as reasonably practicable.

3.2   Customer Data that contains unresolved Exclusions shall be excluded from the Services.

4.   Rejection of Customer Data

4.1   Any Customer Data submission that does not comply with the applicable Data Interface Specification or is in breach of paragraph 1.4 hereof shall be rejected and Customer shall be notified as such.

4.2   Without prejudice to any other remedies that may be available in the circumstances, Customer not delivering Customer Data to IHS Markit that is compliant with the Data Interface Specification may result in Customer and its Underlying Customers (if applicable) not receiving the full functionality of the Services or any Services at all.

5.   Resolving Excluded and Rejected Customer Data

5.1   If the Customer Data in respect of a Business Day contains Exclusions or is rejected in accordance herewith, then:

   (a)   in the case of otherwise compliant Customer Data that contains Exclusions, Customer must provide sign-off or corrections (as applicable) to all such Exclusions as soon as reasonably practicable and following receipt of such revised Customer Data with corrections and sign-offs included, IHS Markit shall repeat such threshold analysis and again identify any remaining unresolved Exclusions; or

   (b)   in the case of Customer Data that has been rejected in accordance herewith, IHS Markit shall use the Customer Data most recently received from Customer that was compliant in the production of the Services (if applicable).

IHS Markit will repeat this process one more time, after which IHS Markit may exclude Customer from the Services until Customer again delivers Customer Data that is compliant.

5.2   It shall be a continuing obligation of Customer to provide sign-off or correction for all Exclusions identified and compliant Customer Data in place of any rejected Customer Data received during the term of the Agreement including any renewal thereof.

5.3   Where IHS Markit and Customer so agree in writing, including as to any applicable fees in respect thereof, IHS Markit shall rectify or cleanse Customer Data received so as to render such Customer Data compliant with the Data Interface Specifications. Otherwise data rectification and cleansing shall be the sole responsibility of Customer.

6.   Future shortening of timescales

6.1   IHS Markit may in the future wish to shorten the data delivery and sign off process set out herein; however doing so would require decreasing the processing time in respect of the Customer Data and also a decrease in the period before Customer Data is submitted. Therefore if IHS Markit notifies Customer that it has been able to decrease the time needed for the processing of the Customer Data, Customer shall correspondingly use its reasonable efforts to move up the applicable deadlines for Customer Data submission as appropriate, all subject to written agreement between the parties from time to time.

EXHIBIT C

IHS MARKIT INFORMATION SECURITY TERMS

These IHS Markit Information Security Terms ("**Information Security Terms**") constitute the information security terms with which IHS Markit shall use its reasonable efforts to comply in the course of providing the Services to Customer under the Agreement. Terms not otherwise defined herein shall have the meaning set out in the Agreement.

1.   General

IHS Markit shall:

1.1   Appoint and notify Customer of the employee of IHS Markit who is to be IHS Markit's contact person in relation to Customer with regard to these Information Security Terms, who shall be responsible for:

> (a)   controlling and coordinating the implementation of these Information Security Terms; and

> (b)   responding to Customer's reasonable inquiries regarding computer and information security.

1.2   Establish and implement appropriate information security policies, processes and procedures aligned to the information security management system standard known as ISO27001. IHS Markit must follow a documented management approval process to handle exceptions and updates to these policies, processes and procedures, taking into account the criticality of the services and processes involved, any changes thereto and reassessment of the risks presented by provision of its Services to Customer from time to time.

1.3   Establish and implement an appropriate and ongoing training and awareness programme to communicate the policies, processes and procedures referred to at paragraph 1.2 above to its employees and contractors. This programme should cover the risks presented by the different types of information to which such employees and contractors may have access and be appropriate in relation to such risks. Attendance and understanding of such programme is to be documented and employees must certify their awareness of and compliance with such policies, processes and procedures. Material breach of such policies, processes and procedures by a IHS Markit employee shall result in disciplinary action.

1.4   Monitor, on a regular basis, reputable sources of computer security vulnerability information such as FIRST, CERT/CC, and mailing lists, taking appropriate measures to obtain, test, and apply relevant service packs, patches, and upgrades to the software and hardware components used by IHS Markit in providing the Services.

1.5   Test, on at least an annual basis, the implementation of these Information Security Terms through the use of network, system, and application vulnerability scanning tools and/or penetration testing.

1.6   Contract, on at least an annual basis with a reputable information security consulting firm to perform application vulnerability scanning, and penetration testing. The results of each assessment and a plan for resolving any problems discovered in a timely manner will be available upon request to Customer within a reasonable period following such request.

1.7   Permit Customer to perform, at the expense of Customer, up to two (2) additional security assessments per year, including but not limited to the areas listed at 1.6 above, upon reasonable advance notice during business hours and to be conducted so as to minimise any business disruption to IHS Markit.

1.8   Establish and implement appropriate fraud prevention and detection controls where Customer's information or other resources to which IHS Markit's employees may have access could potentially be used for fraudulent purposes.

1.9   Take reasonable steps to check the background of IHS Markit's employees who will have access to personal or confidential information in accordance with local laws, including verification of identity and qualifications and obtaining and checking validity of references.

1.10   Implement appropriate authorisation/password controls to prevent unauthorised access to Customer's information. Passwords shall be of an appropriate strength and password-sharing shall be prohibited.

1.11   Maintain, for a period of at least one hundred eighty (180) days (or such longer period as may be required by law or contract) detailed logs files concerning all activity on IHS Markit's relevant systems used in the course of providing the Services, including:

> (a)   all sessions established;

> (b)   information related to the reception of specific information from a user or another system;

> (c)   failed user authentication attempts;

> (d)   unauthorised attempts to access resources (software, hardware, data, processes, etc.);

> (e)   administrator actions; and

> (f)   events generated (e.g., commands issued) to make changes in security profiles, permission levels, application security configurations, and/or system resources.

1.12   Protect all log files against modification, deletion, or unauthorised access. IHS Markit must provide Customer with access to Customer-specific logs upon request.

2.   Network and Communications Security IHS Markit shall:

2.1   Deploy multiple layers of defence on IHS Markit's systems including firewalls, network intrusion detection, and host-based intrusion detection systems. All security monitoring systems, including firewalls and intrusion detection systems, must be monitored twenty-four (24) hours per day, three hundred and sixty-five (365) days per year.

2.2   Notify Customer as soon as commercially feasible and provide Customer, within 5 days of the closure of the incident, if an incident takes place that involves the systems, employees or software used to provide goods and/or services to Customer and provide Customer with a written report describing the incident, actions taken during the response, and plans for future actions to prevent a similar incident from occurring in the future.

2.3   Configure its firewalls, network routers, switches, load balancers, name servers, mail servers, and other network components in accordance with industry best practices.

2.4   Where Customer so requests upon reasonable grounds, and based upon information received by Customer about specific and realistic vulnerabilities and threats, to restrict access within IHS Markit to any Customer-specific component (if any) of IHS Markit's networks, systems, and applications used to provide the Services.

2.5   Deploy firewalls, filtering routers, or other similar network segmentation devices between networks providing services anticipated by this agreement and other IHS Markit networks to control network traffic and minimise exposure to a network compromise.

3.   Infrastructure Platforms, Services, and Operations Security IHS Markit shall:

3.1   Take commercially reasonable steps to ensure all infrastructure platforms, authentication mechanisms, operating systems, web servers, database servers and the like that are used to provide the Services are configured and utilised according to what IHS Markit considers in its reasonable opinion to be industry best practices.

3.2   Ensure that all remote administrative access to production systems in relation to the Services is performed over encrypted connections (SSH, SCP, SSL-enabled web-management interfaces, and VPN solutions) and utilises strong authentication mechanisms.

3.3   Restrict access to each system used to provide the Services to those IHS Markit employees with a job-related need to access such system. Use mechanisms in relation to such restrictions of access that are commensurate with potential threats.

4.   Application Security IHS Markit shall:

4.1   Permit only authenticated and authorised users to view, create, modify, or delete information managed by applications used in connection with providing Services.

4.2   Ensure that web browser cookies, temporary files, and other client-side files that store confidential or personal information are encrypted using a high grade (where permissible) public and widely accepted as secure encryption algorithm. This encryption will be performed independently of any transport encryption such as Secure Sockets Layer. All other cookies must be opaque.

4.3   "Time out" and terminate system communication sessions after an appropriate and reasonable period of user inactivity.

4.4   Where it is reasonably possible to detect such events, terminate any active sessions interrupted by power failure, system "crash," network/connectivity problems, or other apparent anomalies.

4.5   Validate all input and output prior to use to avoid data-driven attacks such as "cross-site scripting" and "SQL injection."

5.   Data Security IHS Markit shall:

5.1   Store and transmit all Customer's confidential information using an appropriate encryption algorithm and cryptosystem.

5.2   When database storage is required, store all Customer's personal information (if any) in a logically or physically separate database that is not shared with other IHS Markit customers, and store all Customer's confidential information in a secure and encrypted form.

5.3   Take steps to protect Customer's information created or transmitted as part of on-line access or transfer so as to minimise the risk of incomplete transmission, misrouting, unauthorised message alteration or duplication, unauthorised disclosure or replay, or other unauthorised or fraudulent activity

5.4   Maintain separate and distinct development, test and staging, and production databases to ensure that production information is not accidentally altered or destroyed.

5.5   Restrict access to any Customer Data to those IHS Markit employees with a job-related need to access such Customer Data. Use mechanisms commensurate with potential threats to such Customer Data.

5.6   Dispose of Customer's confidential or personal information from any system or media no longer in use by IHS Markit securely, by using paper shredders, CD/DVD shredders, and such multi-pass wipe magnetic disk software as may be appropriate for the media/information of concern.

6.   Malicious Code and Virus Protection

6.1   Use and maintain the latest commercially available virus and malicious code detection and protection product(s) on all workstations and servers used to provide the Services.

6.2   Report all occurrences of viruses and malicious code, not handled by deployed detection and protection measures, on any workstation or server used to provide Services, to Customer as soon as reasonably practicable after discovery.

7.   Laptops, Electronic Devices and Storage Devices and Media

7.1   In the event that IHS Markit uses laptops or any other electronic device or media holding Customer's information (including but not limited to USB mass storage devices), IHS Markit shall ensure that:

(a)   any of Customer's confidential or personal information stored thereon shall be encrypted using a mutually agreed upon encryption algorithm and cryptosystem, or in the absence of such agreement, such encryption algorithm and cryptosystem as IHS Markit shall consider appropriate in its reasonable opinion;

(b)   no IHS Markit owned or controlled device shall be connected to a network of Customer without:

(i)   the prior written consent and certification of Customer's relevant department; and

(ii)   such devices employing an operating system approved by Customer (or in the absence of such express approval, Windows 2000 Professional or Windows XP Professional), such operating system to be regularly updated;

(c)   such devices shall be configured with a commercially available anti-virus product (e.g., Norton AV or McAfee), which must be updated on a daily basis (or more frequently if necessary). Such software will be configured in a manner that causes automatic, on-access scanning of the default file types as specified by the anti-virus vendor to be active and periodic scanning of system files. Anti-virus scanning shall not be disabled under any circumstances other than for required maintenance tasks that cannot be conducted without such disablement and in any event a system scan shall be performed upon enablement; and

(d)   browsers, if present, will be current versions of software. Such software shall be regularly updated. Security settings shall not be lowered from the installed defaults.

7.2   Customer may demand the removal from its premises of any IHS Markit device that does not comply with the aforegoing, as well as the user of such device.

8.   Internet Connections on Customer's Premises

8.1   If IHS Markit connects to the Internet from Customer's network while on Customer's premises, it will only do so through Customer's secure gateways. In the event Customer elects to permit IHS Markit's employees and other personnel working on Customer's premises to connect to the Internet via a network that is not managed by Customer, IHS Markit must first seek approval from Customer's relevant and duly authorised department prior to implementing such connection. Any such network connection must utilise content filtering/web filtering software that blocks access to pornographic sites, gambling sites, or other Internet sites that contain any content that is defamatory, offensive or otherwise inappropriate for the workplace and should never be used to bridge Customer's network.

9.   Processing of Personal Information

9.1   This paragraph 9 of the Information Security Terms comprises requirements in relation to the processing of any "personal information" (as defined in the Data Protection Act 1998) which is subject to any law or regulation implementing European Union Directive 95/46/EC, where this is applicable. IHS Markit and Customer agree that the Services are not anticipated to involve any processing of personal information, but acknowledge that if any personal information is ever processed in the course of providing the Services, the IHS Markit Policy for the Processing of Data Governed by the GDPR shall apply and is located at https://ihsmarkit.com/Legal/data-governed-gdpr.html.

9.2   Where Customer is obliged by law or regulations, or the rules of a regulatory authority to which Customer is subject, IHS Markit shall disclose the results of the security assessments referred to in these Information Security Terms to a regulator (including national data protection authorities) IHS Markit hereby consents to such disclosure.

9.3   IHS Markit shall ensure that:

(a)   only authorised IHS Markit employees with job-related needs access any personal information in the course of providing goods and services under the Agreement (and such personal information cannot be read, copied, modified or removed without authorisation, either in the course of processing or use or after storage);

(b)   such access is only given to such authorised staff to the extent necessary for the performance of their duties;

(c)   an up-to-date list is kept of such authorised staff and their level of authorised access (and authorisation credentials are checked at least on an annual basis);

(d)   personal information collected for different purposes can be processed separately; and

(e)   a documented procedure is put in place to control access by authorised users under which each user is provided with a particular identification code that cannot be assigned to any other user at any time, while passwords:

     (i)   are at least eight characters long (or less, but only if the password is as long as the maximum number of characters allowed by the electronic device involved),

     (ii)   do not contain any clear reference to the user, and

     (iii)   are changed after the first access and periodically, at least every six (6) months, or disenabled if they are not used for six (6) months or if the means necessary to access personal information are lost (and in each case, if the user has access to Sensitive Personal Data the six (6) month period is reduced to three months).

Such passwords shall be kept secret/confidential and not shared or otherwise disclosed whilst still valid.

9.4   IHS Markit shall ensure that the identification and verification of authorised users is implemented in such a way that the risk of an error occurring is minimised, and impose industry-standard limits designed to prevent attempts to obtain unauthorised access.

9.5   IHS Markit shall ensure that such authorised employees are provided with mandatory policies governing their access to such personal information, such mandatory policies to be regularly updated.

9.6   IHS Markit shall ensure that personal information cannot be read, copied, modified or removed without authorisation during electronic transmission or transport, and that it is possible to check and establish to which bodies personal information is to be transferred by means of data transmission facilities.

9.7   IHS Markit shall keep a register of any incident which may affect the security of such personal information, such register to be made available to Customer upon request. For each security incident registered, the register must include the following information:

(a)   the time at which the incident occurred;

(b)   the person reporting it;

(c)   to whom it was reported;

(d)   the consequences thereof; and

(e)   the procedures put in place to recover any personal information (indicating the person who undertook the process, the information recovered and, if appropriate, which data items had to be input manually as part of the recovery process).

9.8   IHS Markit shall not implement any data recovery procedures in relation to personal information unless it has obtained written authorisation from Customer.

9.9   IHS Markit shall ensure files containing personal information which are handled manually shall comply with appropriate security measures, and, will be subject to the following measures:

(a)   adequate archiving of the media or documents containing personal information (so that document conservation, location and information look-up is guaranteed and privacy rights of individuals are preserved);

(b)   storing devices incorporate mechanisms which make its opening difficult;

(c)   appropriate protection of media or documents containing personal information is effected prior and consequent to its archiving so that unauthorised access is prevented at all times;

(d)   cabinets or other storing elements shall have access doors with a key or equivalent device;

(e)   copies of documents will solely be done under the control of authorised staff;

(f)   discarded copies shall be destroyed; and

(g)   access or manipulation of such files will be impeded during their transportation.

9.10   IHS Markit shall ensure that, if applicable, any IHS Markit employee is authorised to access personal information in the course of providing the Services and that it can be checked and established whether and by whom personal information has been input into IHS Markit's data processing systems, modified or removed.

9.11   IHS Markit shall ensure that, if any personal information is to be processed in the coming year, a security measures document is created or updated by 1 March in such year, identifying the relevant personal information file and data treatment and specifying:

        (a)   the security measures to be implemented with regard to the provision of Services;

        (b)   an analysis of the risks run in the data processing;

        (c)   the data recovery procedures; and

        (d)   the training programs aimed at the employees who process the personal information.

9.12   IHS Markit shall ensure that the use of portable devices storing personal information are previously authorised by Customer and in any case the applicable security measures are applied.

9.13   IHS Markit shall ensure temporary files have a level of security appropriate to the type of personal information contained therein. All temporary files must be erased once they are no longer necessary for the purposes for which they were created.

9.14   Security measures required for access to personal information via communications networks or when processing personal information outside the premises where the personal information is located (e.g. via remote access) must have a security level equivalent to that applying to local access.

9.15   Where the Services involve processing of personal information, IHS Markit shall perform backups of all systems, applications, and data used to provide such Services at least weekly.

9.16   The back up and data recovery procedures must guarantee the reconstruction of any personal or confidential information involved to the state they were in at the time they were lost or destroyed.

9.17   The back up and data recovery procedures described in this paragraph 9, to the extent applicable, must include a regular testing schedule.

10.   Processing of Sensitive Personal Data

10.1   This paragraph 10 shall apply to "**Sensitive Personal Data**" being personal information revealing or concerning (directly or indirectly) racial or ethnic origin, political affiliations or opinions, religious or philosophical beliefs, trade-union membership or membership of other parties, associations or organisations of a religious, philosophical, political or trade-union nature, physical or mental health or condition including addictions, sex life, private life, social aid, the commission or alleged commission of any criminal offence or proceedings in relation thereto, other criminal behaviour or unlawful or objectionable conduct, administrative proceedings and sanctions and other judicial data.

10.2   Any transport of hardware or other physical media containing Sensitive Personal Data may only be carried out after such Sensitive Personal Data have been encrypted, using an appropriate encryption algorithm and cryptosystem.

10.3   Any transfer of Sensitive Personal Data via any telecommunications system or network may only be carried out after such Sensitive Personal Data have been encrypted, using an appropriate encryption algorithm and cryptosystem.

10.4   Each access to Sensitive Personal Data (whether manual or electronic) must be recorded indicating:

        (a)   the date and time;

        (b)   the identity of the user;

        (c)   the file to which the user has had access;

        (d)   the kind of access (e.g. read only); and

        (e)   whether the access has been authorised or refused.

Such record must be kept for at least two (2) years from the date it is entered. IHS Markit shall make such record available to Customer upon reasonable request and shall additionally submit a summary report of the access record on a monthly basis to Customer.

10.5   Back up copies shall be made of the Sensitive Personal Data and stored at a location which is different to the location where the Sensitive Personal Data are located, such storage to comply with the security requirements set out in these Information Security Terms. If the Sensitive Personal Data is taken off site, it shall be encrypted using an agreed encryption algorithm and cryptosystem.

10.6   Any maintenance on devices that store, or previously stored, Sensitive Personal Data, which requires the media to be removed from site must ensure that data is cleansed, or wiped, using the agreed cleaning process.

11.   Physical Security

IHS Markit shall:

11.1   Maintain all workstations, servers, and active and passive network equipment used to provide Services (including to store back-up copies) in secure facilities owned, operated, or contracted for by IHS Markit so that unauthorised persons are not provided with access.

11.2   Limit access to these secure facilities to:

(a)   authorised IHS Markit employees with job-related needs; and

(b)   visitors who may have a legitimate need to access the facilities, but such visitors shall only be permitted to access public areas or otherwise shall be supervised by IHS Markit employees.

11.3   Monitor access to these secure facilities through the appropriate use of security guards, surveillance cameras, security alarms and lighting, authorised entry systems, or similar methods capable of recording entry and exit information.

11.4   Secure all laptops and other portable electronic devices and media (e.g. PDAs, disks, memory sticks) and hard copy (e.g. paper-based) records which contain Customer confidential information appropriately e.g. lock up overnight or when otherwise not in use.

11.5   Securely transport all media (including back-up and archival media) containing Customer's confidential or personal electronic information or other electronic information used to provide the Services using an appropriate encryption algorithm and cryptosystem. Hard copy (paper-based) records including such information shall also be securely transported (e.g. by courier).

11.6   Maintain all backup and archival media containing Customer's information, or other information used to provide goods and/or services under this Agreement, in secure, environmentally-controlled storage areas owned, operated, or contracted for by IHS Markit. Limit access to backup and archival media storage areas and contents to authorised IHS Markit employees with job-related needs.

11.7   Document and implement appropriate procedures requiring the inventory, control and recording of any movement of any such equipment, device or media containing Customer's information on/off the secure facilities mentioned above.

11.8   Maintain a register of the arrival and removal of computer hardware to/from the secure facilities and storage areas mentioned above.

11.9   Ensure media containing personal information indicate the type of information they contain and are located in secure facilities with restricted access and listed on a register to be maintained by IHS Markit. Additionally, such register must contain details of the entry and exit to/from such facilities of media containing personal information. This register must permit direct or indirect identification of the kind of media involved and list:

(a)   the date and time;

(b)   the sender/receiver;

(c)   the number of media;

(d)   the kind of information contained therein;

(e)   how they are sent/received; and

(f)   the person responsible for sending/receiving them who must be duly authorised.

The removal of media containing personal information outside of the secure facilities where the database containing such personal information is located shall only be permitted with Customer's prior written authorisation.

11.10   Ensure that where personal information from any system or media no longer in use for the provision of Services to Customer are disposed of in accordance with these Information Security Terms, the personal information that has been disposed of shall be withdrawn from the register.

12.   Business Continuity Plan

12.1   The parties have implemented and shall periodically test and at all times maintain a business continuity and disaster recovery plan ("**Business Continuity Plan**") in an effort to minimise the risk of any interruption in the delivery of the Services or the Customer Data (as applicable) and in the event of such interruption, aim to recommence delivery of Services or Customer Data (as applicable) as quickly as circumstances allow, in accordance with the relevant Business Continuity Plan, in the event of a power outage, systems outage, major disaster or other circumstance severely interrupting normal business, regardless of cause. The Business Continuity Plans must include the following:

(a)   A clear definition of and strategy for meeting recovery time objectives (RTO) and recovery point objectives (RPO) (where applicable) for each business location associated with providing the Services or the Customer Data (as applicable).

(b)   Maintenance of a geographically diverse recovery/backup location that is not dependant, to the extent practicable, on the same critical infrastructure as the primary location to minimise the probability that both facilities will be affected by the same event. Such location must maintain similar levels of physical and access security controls to those maintained at the primary site.

(c)   Documentation that the Business Continuity Plan's business continuity provisions can continue to provide the Services or the Customer Data (as applicable) through a scenario involving loss or loss of use of the primary facility and a significant proportion of its employees based in such location.

(d)   Procedures for Business Continuity Plan invocation, activation of the recovery site(s) and notification of all employees, suppliers, contractors, customers and service providers of the invocation of the Business Continuity Plan.

(e)   Identification of all mission critical systems, external dependencies, network diversity, vital records, personnel and the provisions in place to ensure their availability.

(f)   Procedures to perform backups of all systems, applications, and data used to provide the Services or Customer Data (as applicable) in a manner designed to ensure their availability in the event of a disaster. Such procedures must include the periodic transfer of backup media to a secure off-site storage facility.

(g)   A schedule for periodically testing and at all times maintaining the Business Continuity Plan and a procedure for incorporating any identified shortcomings of the Business Continuity Plan that become apparent from tests into the next scheduled Business Continuity Plan revision.

(h)   Evidence the Business Continuity Plan has been approved by the relevant party's executive management.

(i)   Identification of any applicable regulatory issues affecting the BCP.

12.2   Each of the parties shall:

(a)   notify the other of any activation of the Business Continuity Plan within 24 hours following activation, and in the event of any interruption or degradation of Services or the Customer Data, provide regular status updates at appropriate intervals to the other for the duration of the recovery period;

(b)   provide to the other the names of any key individuals to be contacted during any activation of the Business Continuity Plan (including office, home, mobile and pager numbers for 24x7 communications).

(c)   notify the other of any material changes to the Business Continuity Plan or to their recovery capability that could adversely affect the delivery of the Services or Customer Data (as applicable);

(d)   notify the other of the results of any scheduled tests of the Business Continuity Plan that require changes to the Business Continuity Plan, and of such party's proposed changes and the timescale for implementation thereof.