RPM STANDARD TERMS AND CONDITIONS
("Terms and Conditions")

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 Terms and Conditions, including the Schedules hereto;

"**Booking Form**" means the document entitled "Research Payment Accounts Manager Services Booking Form" signed by Subscriber incorporating these 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;

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

"**Fees**" means the fees for the Services payable by Subscriber 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, trade marks, 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 Markit attached hereto and identified as Exhibit B;

"**Log-on**" means the unique user name and password details provided hereunder to Subscriber enabling access to those Services available through the RPM Manager;

"**Markit**" means Markit Group (UK) Limited or its Affiliate(s);

"**Outputs**" means such information (in whatever medium) as is provided to Subscriber by Markit as part of the Service that are provided through the RPM Manager or made available for Subscriber 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;

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

"**RPM Manager**" means a hosted, web-based application provided by Markit to allow the Subscriber to access the Services using its unique Log-on to manage its acquisition of research across its research payment accounts as further described in Exhibit A – Services Schedule;

"**Services**" means such services of those described in the Services Schedule as are to be received by Subscriber from 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

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

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

"**Subscriber Data**" means Subscriber's research payment account data to be delivered to Markit pursuant to this Agreement;

"**Subscriber Instructions**" means Subscriber's research payment account instructions to be delivered by Subscriber to Markit pursuant to this Agreement;

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 Markit

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

2.2 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 Markit warrants it is appropriately authorised to provide the Services to Subscriber and that it has such relevant rights, consents and licences as may be required to enable it to do so.

2.4 Markit shall use reasonable efforts to ensure that the RPM Manager shall be in good operating condition.

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

2.6 Markit shall provide Subscriber access to the Services and the RPM Manager as of the Commencement Date or such other date as set out in the Booking Form.

3. Obligations of Subscriber

3.1 Subscriber shall:

(a) deliver the Subscriber Instructions to Markit in accordance with the RPM Manager;

(b) ensure that each Log-on provided to Subscriber by 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 Markit, immediately, if a Log-on is to be revoked.

3.2 Subscriber 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 Markit of Subscriber Instructions, the receipt and analysis of Outputs or other Deliverables and any other matter related to the Services.

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

(a) supply the Subscriber Instructions to Markit in accordance with this Agreement; and

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

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

3.5 Subscriber must not:

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

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

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

3.7 Subscriber 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 Markit and Subscriber, 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 Ltd. from inception.

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

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

4.4 Markit grants Subscriber a revocable, non-exclusive licence for Subscriber's Permissioned Business Unit to access the Services, RPM Manager and to use and copy the Outputs only for the Permitted Purpose in accordance herewith. Subscriber may not publish Outputs or any information derived from the Outputs in any way other than for the Permitted Purpose. Subscriber 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. Subscriber shall not permit the Services to be used by any other member third party including its Affiliates.

4.5 Subscriber shall only access and use the data as contained in the Services in accordance with (i) the permissions as granted by the relevant subscribers to the Services; (ii) comply with any instructions or permitted uses contained therein; and (iii) comply with any data protection, privacy or similar laws that may apply to the data contained in the Services. Subscriber acknowledges and agrees that the Services are subject to all disclaimers, legends and notices that may be contained therein from time to time.

4.6 Subscriber grants Markit an irrevocable, non-exclusive, royalty-free licence to use the Subscriber Data to generate the RPM Aggregated Data and to provide the Services.

4.7 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 Subscriber shall pay to Markit the Fees set out in the Booking Form.

5.2 Fees shall be invoiced by 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 Subscriber must pay these to 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, Markit may invoice Subscriber for such tax and Subscriber shall pay such invoice as set forth above.

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

(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 Subscriber Data in accordance with its obligations hereunder.

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

6. Use of the Services

If Markit reasonably believes that Subscriber is permitting use of any Deliverable, Log-on or Output otherwise than in accordance herewith, Markit shall notify Subscriber, and Subscriber shall promptly use its best efforts to ensure any such use ceases. Markit may suspend the Services to Subscriber 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, Subscriber 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 recipient of Confidential Information'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 recipient of Confidential Information's auditors or lawyers; or

(c) any temporary staff, contractors or consultants working for the recipient of Confidential Information 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) available to any counterparty or payment agent permissioned via the Services by Subscriber to access, view, or download information provided by Subscriber;

(d) made available to any third party vendor under confidentiality agreements for the purpose of improving or disseminating the Services;

(e) trivial or obvious; or

(f) 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 compliance by Subscriber with Clause 8.3, Markit shall indemnify Subscriber against each loss, liability and cost (including reasonable legal costs and attorneys' fees) that Subscriber incurs or becomes liable for arising out of: i) a claim of infringement of an Intellectual Property Right howsoever arising as a result of or in connection with the use of the Services by the Subscriber in accordance with this Agreement; or ii) any breach of Section 7 (Confidentiality) above, (including, without limitation, each loss, liability and cost incurred as a result of defending or settling such claim).

8.2 Subject to compliance by Markit with Clause 8.3, Subscriber shall indemnify Markit against each loss, liability and cost (including reasonable legal costs and attorneys' fees) that Markit incurs or becomes liable for arising out of: i) a claim of infringement of an Intellectual Property Right howsoever arising as a result of or in connection with the receipt or use of the Subscriber Data or any part of it in accordance with this Agreement; or ii) any use of a Service in breach of the terms of this Agreement or a breach of Section 7 (Confidentiality) above, (including, without limitation, each loss, liability and cost incurred as a result of defending or settling such claim);

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) each party's obligations under Sections 7 and 8;

(d) fraudulent misrepresentation; or

(e) 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 Subscriber in respect of the year in which the relevant liability arises.

9.4 Subscriber recognises that the Outputs (and any other Deliverables) are performance analysis tools designed to assist in the making of investment and research decisions and the management of securities portfolios, but that Subscriber shall have and bear sole and complete responsibility for all such decisions and management. Accordingly, 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 Subscriber 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 Subscriber warrants and represents to Markit that: (a) where Subscriber supplies to Markit information belonging to a third party, Subscriber has obtained the necessary consents and authority in order to use such information in the Services; and (b) Subscriber's use or intended use of the Services shall not violate any applicable local, state, national or international law, statute, ordinance, rule or regulation, relating to competition or antitrust.

9.6 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).

9.7 MARKIT DOES NOT GUARANTEE THE ACCURACY AND/OR THE COMPLETENESS OF ANY OF THE SERVICES SUPPLIED BY IT OR ANY INFORMATION INCLUDED THEREIN. MARKIT MAKES NO WARRANTY, EXPRESS OR IMPLIED, AND EXPRESSLY DISCLAIMS ALL WARRANTIES AS TO RESULTS TO BE OBTAINED BY SUBSCRIBER OR ANY OTHER PERSON OR ENTITY FROM THE USE OF THE SERVICES SUPPLIED BY MARKIT OR ANY INFORMATION INCLUDED THEREIN. 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 SERVICES SUPPLIED BY MARKIT OR ANY INFORMATION INCLUDED THEREIN. WITHOUT LIMITING ANY OF THE FOREGOING, IN NO EVENT SHALL MARKIT HAVE ANY LIABILITY FOR ANY SPECIAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS), EVEN IF NOTIFIED OF THE POSSIBILITY OF SUCH DAMAGES.

9.8 Subscriber agrees that Markit shall not assume responsibility for verification, completeness, timeliness or

accuracy of data provided and shall not be responsible or liable for any errors, factual or otherwise, contained in any data in the Services whether provided by Subscriber or any third party. Neither Markit nor any other person (including without limitation any person or entity that has participated in any respect in the development or collection of the Services (each a "**Data Provider**")) makes any representation or warranty as to any Services. Neither Markit nor any Data Provider shall have any liability, duty or obligation for or relating to the Services or the data contained therein, or for any errors, inaccuracies, omissions or delays in content, or for any actions taken in reliance thereon.

9.9 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, Markit shall have no liability or responsibility to Subscriber for the quality, functionality or any other aspect of such service, or the accuracy, timeliness or completeness of Outputs received by Subscriber through such service, and Subscriber shall be solely responsible for maintaining a services agreement directly with the provider of such service for usage of Outputs. Subscriber 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. Acknowledgement

Subscriber agrees that: (a) Markit does not owe Subscriber any duty to monitor or enforce compliance by any other subscriber with any provision, regulation or law with relates to its use of the Services; (b) Markit does not warrant that by subscribing for the Services Subscriber shall be deemed compliant with any applicable rules, regulations or laws; (c) as per Section 9.8 above, Markit has no responsibility for verifying, correcting, or updating any electronic instructions or information sent from Subscriber. As such, Subscriber agrees that it is responsible for ensuring that all information supplied to Markit in its use of the Services is up to date, and will ensure that it has appropriate measures in place to ensure that such information is updated when required; (d) Markit does not undertake any responsibility towards any person on whose behalf Subscriber is acting on and Subscriber is responsible for advising such person of any such matter and obtaining any requisite permission; (e) As part of the Services, Markit may at Subscriber's permission make certain Subscriber's data available to third parties as nominated by Subscriber. Markit shall be entitled without further enquiry to execute or otherwise act upon any instructions or information or purported instructions or information received by or in connection with the Services notwithstanding that it may afterwards be discovered that any such instruction or information was not genuine or not correct or not sent with authority; (f) Subscriber will ensure that it transmits electronic instructions to Markit is fully and validly authorized to do so and ensure that all material it sends to Markit during the use of the Services is accurate; and (g) Markit shall be entitled to extract data from the Services for usage on an anonymised basis.

11. Transition Services

11.1 Subscriber Data in the Services shall kept by Markit for up to seven (7) years during the Term. Subscriber Data shall be treated as "Confidential Information" and Markit shall not own any data provided by Subscriber. At the end of the Term, Markit may make a download made available of Subscriber's available trades and payment data (if requested).

12. Term and Termination

12.1 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 12. 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 12.3.

12.2 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 12.2(b) to (g) inclusive.

12.3 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.

13. Consequences of Termination

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

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

13.3 The provisions of Clauses 1 (Definitions and Interpretation), 4.1, 4.2, 4.3, 4.5 and 4.7 (Intellectual Property and Licence), 6 (Use of the Services), 7 (Confidentiality), 8 (Indemnities), 9 (Exclusions and Limitations), 13 (Consequences of Termination) and 14 (General) shall survive any expiry or termination of this Agreement and shall remain in full force and effect.

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, Markit may update these Terms and Conditions, including by way of example the descriptions of Services in the Services Schedule and the contents of the Information Security Terms, from time to time by amending such Schedule, uploading the amended Markit Terms and Conditions to the relevant website and notifying Subscriber 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 Subscriber 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 Terms and Conditions;
(c) the Services Schedule; and finally
(d) 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 14.3, provided that no notice to Markit shall be effective unless a copy has been sent to the attention of Markit's Legal Team at 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 Markit may

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

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

provided that in each case Markit shall remain ultimately responsible to Subscriber for Markit's obligations hereunder. Further, Markit may assign its rights under this Agreement in connection with the sale of all or substantially all of the shares or assets of 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 Subscriber 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 and each party submits to the exclusive jurisdiction of the courts residing in New York, New York, USA; otherwise this Agreement shall be governed by the laws of England and Wales and each party submits to the exclusive jurisdiction of the courts residing in London, England, United Kingdom for the purposes of determining any dispute arising out of this Agreement or the transactions contemplated by them. Regardless of jurisdiction, in each case without regard to any conflicts of laws principles.

EXHIBIT A

SERVICES SCHEDULE

This Services Schedule ("**Services Schedule**") constitutes a description of Markit's Research Payment Account Manager. The Services that Subscriber 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 Research Payment Manager

1.1 Markit will provide the Research Payment Manager, which will include the following functionality:

1.1.1 Database of research providers and their service descriptions.

1.1.2 Budgeting and allocation of research services at multiple levels (including firm, investment team and portfolio manager) based upon flexible budgeting periods:

- Users will be able to establish research service budgets at various organizational levels: the enterprise, investment team/strategy or portfolio manager;
- Budgets can be allocated across portfolios based on a pre-determined allocation factor; and/or
- Budgets can be dynamically re-allocated as events dictate.

1.1.3 Funding of research payment accounts through:

- direct payments from the underlying client portfolios;
- sweep of research credit balances accumulated with brokers (through the use of CM); or

1.1.4 Payment recording management for invoiced and non-invoiced services, partial payment and mixed use services.

1.1.5 Recording of details of all invoices, including a scanned image of the physical document.

1.1.6 Segregation of eligible payments from non-eligible.

1.1.7 Implementation of between one and ten levels of internal payment authorization.

1.2 The RPM Manager offers standardized disclosure and regulatory reports, as well as the ability to run flexible reports, charts, dashboards and data extracts that cover budgeting, funding, and payments.

1.3 For greater clarity, in respect of the RPM, Subscriber acknowledges and agrees:

1.3.1 In the case of a RPM, the Subscriber funds will be in a segregated account that is held at a custody bank; and

1.3.2 Markit will act as a payment *facilitator*, however the Subscriber will be responsible for directing payments.

EXHIBIT B

MARKIT INFORMATION SECURITY TERMS

Commented [INFO1]: Are these InfoSec terms still accurate for the new RPM/M service?

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

1. General

Markit shall:

1.1 Appoint and notify Subscriber of the employee of Markit who is to be Markit's contact person in relation to Subscriber 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 Subscriber'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. 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 Subscriber 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 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 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 Subscriber within a reasonable period following such request.

1.7 Permit Subscriber to perform, at the expense of Subscriber, 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 Markit.

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

1.9 Take reasonable steps to check the background of 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 Subscriber'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 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. Markit must provide Subscriber with access to Subscriber-specific logs upon request.

2. Network and Communications Security

Markit shall:

2.1 Deploy multiple layers of defence on 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 Subscriber as soon as commercially feasible and provide Subscriber, 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 Subscriber and provide Subscriber 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 Subscriber so requests upon reasonable grounds, and based upon information received by Subscriber about specific and realistic vulnerabilities and threats, to restrict access within Markit to any Subscriber-specific component (if any) of 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 Markit networks to control network traffic and minimise exposure to a network compromise.

3. Infrastructure Platforms, Services, and Operations Security

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 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 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

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

Markit shall:

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

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

5.3 Take steps to protect Subscriber'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 Subscriber Data to those Markit employees with a job-related need to access such Subscriber Data. Use mechanisms commensurate with potential threats to such Subscriber Data.

5.6 Dispose of Subscriber's confidential or personal information from any system or media no longer in use by 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 Subscriber as soon as reasonably practicable after discovery.

7. Laptops, Electronic Devices and Storage Devices and Media

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

(a) any of Subscriber'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 Markit shall consider appropriate in its reasonable opinion;

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

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

(ii) such devices employing an operating system approved by Subscriber (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 Subscriber may demand the removal from its premises of any Markit device that does not comply with the aforegoing, as well as the user of such device.

8. Internet Connections on Subscriber's Premises

8.1 If Markit connects to the Internet from Subscriber's network while on Subscriber's premises, it will only do so through Subscriber's secure gateways. In the event Subscriber elects to permit Markit's employees and other personnel working on Subscriber's premises to connect to the Internet via a network that is not managed by Subscriber, Markit must first seek approval from Subscriber'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 Subscriber'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. Markit and Subscriber 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, this paragraph 9 shall apply.

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

9.3 Markit shall ensure that:

(a) only authorised 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 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 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 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 Markit shall keep a register of any incident which may affect the security of such personal information, such register to be made available to Subscriber 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 Markit shall not implement any data recovery procedures in relation to personal information unless it has obtained written authorisation from Subscriber.

9.9 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 Markit shall ensure that, if applicable, any 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 Markit's data processing systems, modified or removed.

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

9.13 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, 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. Markit shall make such record available to Subscriber upon reasonable request and shall additionally submit a summary report of the access record on a monthly basis to Subscriber.

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

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 Markit so that unauthorised persons are not provided with access.

11.2 Limit access to these secure facilities to:

(a) authorised 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 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 Subscriber 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 Subscriber'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 Subscriber'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 Markit. Limit access to backup and archival media storage areas and contents to authorised 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 Subscriber'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 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 Subscriber'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 Subscriber 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 Subscriber Data (as applicable) and in the event of such interruption, aim to recommence delivery of Services or Subscriber 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 Subscriber 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 Subscriber 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 Subscriber 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 Subscriber 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 Subscriber 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.