Technical and Organizational Security Measures Implemented by Service Provider

In the event of a conflict between a term of this Exhibit, and a term of the underlying agreement between the Parties (the "Agreement"), the latter shall govern. Service Provider agrees and warrants that it has implemented technical and organizational measures appropriate to protect Confidential Information (including Personal Data) against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation. The measures Service Provider has taken include, as appropriate and without limitation:

1. Information Security Management System

   a. The Service Provider shall implement and maintain an appropriate information security management system ("ISMS"), which shall include written policies and procedures and implemented technical, physical and organizational security controls to:

      i) identify and protect against potential threats to and ensure the security and availability of the Service Provider's IT systems and Confidential Information;

      ii) protect against unauthorized or unlawful processing of Confidential Information and against accidental loss or destruction of, or damage to, Confidential Information; and

      iii) document, without limitation, the security controls specified in this Exhibit**.**

   b. Without limiting the generality of the obligation in Section 1.a, Service Provider shall, at a minimum, implement and maintain the security controls set out in this Exhibit as part of its ISMS.

   c. The Service Provider shall regularly review and, as appropriate, update its ISMS to take into account:

      i) changes in the nature of the Confidential Information and harm that might result from such unauthorized or unlawful processing or accidental loss, destruction or damage of the Confidential Information;

      ii) changes in state of technological development, including without limitation changes to relevant, industry recognized, information security standards; and

      iii) new threats or vulnerabilities relevant to and affecting the Service Provider's IT systems or Confidential Information.

   d. The Service Provider shall maintain appropriate and complete documentation describing its ISMS (including without limitation a log of all changes made to it) and will provide such documentation to McKinsey promptly on request.

2. Designated Information Security Executive

   a. The Service Provider shall appoint a designated security officer ("Security Officer") who shall be responsible for the development, implementation and ongoing maintenance of its ISMS. The contact information for the Security Officer is as set forth in the Agreement.

   b. The Service Provider shall notify McKinsey in the event that it changes its Security Officer and shall provide each new Security Officer's name, phone number and email address.

   c. The Security Officer must be of management level or above, be employed by Service Provider and have appropriate, recognized information security management experience and qualifications. The Service Provider shall promptly provide McKinsey on its request with details of the Security Officer's position

within the management hierarchy of Service Provider and a copy of the Security Officer's information security experience and qualifications. A failure by Service Provider to appoint a Security Officer meeting the requirements of this Section 2.c shall be a material breach of the Agreement.

3. Access Rights

a. Limitation of Access

i) The Service Provider shall limit access to the Service Provider's IT systems and Confidential Information to those Service Provider personnel performing the Services and shall ensure that each of those personnel are properly authorized and are under appropriate written confidentiality and non-disclosure obligations. The Service Provider shall promptly disable or reduce access for personnel who should no longer need their current level of access (including, without limitation, individuals who are no longer employed by the Service Provider).

ii) The Service Provider shall set permission levels at the minimum requirement for relevant user to fulfill his or her approved business role as part of the Service Provider's performance of the Services (concept of least privileged access).

iii) The Service Provider shall implement technical and organizational measures to prevent persons from making copies of or transmitting Confidential Information except to the extent strictly necessary to perform the Services.

b. Authentication

i) Any Service Provider IT system used to access or otherwise process Confidential Information shall use authentication methods which identify a unique user, utilize a strong password, and adequately protect the password via encryption for user and system IDs.

ii) The Service Provider shall use a reasonably secure method of selecting passwords and providing passwords and token devices to Service Provider personnel or use unique identifier technologies (such as biometrics). The Service Provider shall ensure that passwords are kept in a secure location and format and shall ensure that passwords are appropriately encrypted or stored using an appropriate salted hash.

iii) The Service Provider shall ensure that management approval and multifactor authentication is required for administrative user access to Confidential Information or any other systems through which Confidential Information may be accessed. All administrative user sessions should be set to expire within fifteen minutes.

iv) The Service Provider shall promptly notify McKinsey of changes to Service Provider's roster of personnel engaged in the Services involving access to Confidential Information on the Service Provider's, McKinsey's customers, or McKinsey's networks, servers, or applications.

v) The Service Provider shall promptly deactivate individual user IDs and passwords through which access may be made to Confidential Information upon termination of the Services pursuant to which such Confidential Information was provided, termination of said individual's need for access due to role change or termination, or upon written request from McKinsey.

4. Encryption of Confidential Information

The Service Provider shall implement encryption with respect to all records and files containing Confidential Information either at rest or in transit, including without limitation all Confidential Information to be transmitted across public networks or wirelessly. The Service Provider shall implement the following minimum precautions when encrypting Confidential Information:

a. The Service Provider shall use industry standard algorithms that meet or exceed FIPS 197 encryption standard (or the standard that supersedes the FIPS encryption standard) to encrypt Confidential Information.

b. The Service Provider shall ensure that all encryption keys/passwords used to access encrypted Confidential Information shall be stored separately from the encrypted Confidential Information.

c. The Service Provider shall ensure that all network, application, and server authentication passwords meet minimum complexity guidelines (at least 8 characters with at least 3 of the following four classes: upper case, lower case, numeral, special character) and be changed at least every 75 days.

5. Transmission

The Service Provider shall implement the following minimum precautions when transmitting Confidential Information:

a. The Service Provider shall provide a secure file transfer mechanism (encrypted in accordance with Section 4) for upload of Confidential Information to the Service Provider's IT systems.

b. The Service Provider shall prohibit (technically and organizationally) the connection of portable media to the Service Provider's IT system hosting Confidential Information, except as strictly necessary for backup purposes.

c. The Service Provider shall prohibit (technically and organizationally) the connection of devices to the Service Provider's IT system hosting Confidential Information which are capable of printing data to hardcopy.

6. Storage

The Service Provider shall implement the following minimum precautions when storing Confidential Information:

a. The Service Provider shall ensure that Confidential Information uploaded by McKinsey that are stored in the Service Provider's IT systems are encrypted in accordance with Section 4 above.

b. Where Service Provider backs up databases, services or its IT systems and those backups may contain Confidential Information, the backups must be stored in a locked facility, with restricted access to appropriate authorized personnel only and shall be encrypted in accordance with Section 4.a above. All such backups shall be logged, authorized by the Service Provider's Security Officer and sent via secured courier or other delivery method that can be tracked.

c. The Service Provider shall ensure that McKinsey's Confidential Information is not physically comingled with any of the Service Provider's (or any third party's) other data, or virtually co-mingled with other data where such Confidential Information shares the same media, device or system, unless the data is logically separated, or compensating controls, approved by McKinsey, are implemented.

7. Network Security

The Service Provider shall have the following or equivalent capabilities for Service Provider's IT systems:

a. General

The Service Provider shall employ an appropriate layered approach to the security of its IT systems processing Confidential Information (or supporting infrastructure) by separating the various layers of its networks and protecting information exchange boundaries with security gateways to narrow the available communication routes among network layers. The Service Provider shall ensure that appropriately

configured firewalls, VLANs and private IP addressing are deployed to secure communications routes into, out of and between layers within its IT systems.

b. Firewalls/Network Configurations

i) The Service Provider shall ensure that all network traffic in and out of the Service Provider's IT systems shall pass through firewalls deployed to protect the perimeter and every internal layer of the Service Provider's IT systems.

ii) The Service Provider shall ensure that firewalls and routers are configured appropriately to maintain the security and integrity of Confidential Information and that restrict connections among layers of the Service Provider's IT systems and with untrusted networks.

iii) The Service Provider shall ensure that anti-spoofing filters are enabled.

iv) The Service Provider shall establish up-to-date application security firewalls to ensure protection of application platform oriented threats.

c. Administrative Access

The Service Provider shall ensure that access to the Service Provider's IT systems for administration shall be via encrypted virtual private network, subject to appropriate access control lists and shall comply with Sections 3, 4 and 5 above.

d. Intrusion Detection and Logging

i) The Service Provider shall implement and maintain hardware, software, and/or procedural mechanisms that record activity in its IT systems, including without limitation appropriate logs intrusion detection/prevention systems that allow traffic flowing through the firewalls and VLANs to be logged and protected at all times.

ii) The Service Provider shall ensure that such logging and intrusion detection/prevention systems produce regular reports and are regularly reviewed for malicious and unauthorized activity within and potential threats to the Service Provider's IT systems.

iii) All systems shall support general system logging that captures such information as date/time of all authentication events (e.g., login/logout, failed logins). All applications will support logging that captures such information as privileged or administrative user activities (e.g., user creation, user deletion, user modification).

iv) The Service Provider shall engage an independent third-party security firm to conduct penetration tests on Service Provider's IT systems and application platforms no less frequently than once annually.

e. File Integrity

The Service Provider shall implement appropriate file integrity systems to protect the integrity of critical system files and the Confidential Information (including without limitation protection from unauthorized alteration, corruption or destruction of such data).

8. Printed Documents

Any hardcopy documents received or produced by the Service Provider containing Confidential Information must not be disclosed to third parties and shall be protected at all times using physical means and when no longer needed destroyed using, at minimum, a cross cut shredder.

9. Data Disposal

Where Confidential Information is required to be disposed of by McKinsey, including as requested by McKinsey, the Service Provider shall ensure that disposal occurs securely and in accordance with applicable law and industry standards so that the disposed Confidential Information cannot be read or reconstructed.

10. Service Locations

Service Provider shall promptly inform McKinsey on its request, of all locations at which McKinsey's Confidential Information may be stored or processed and shall promptly notify McKinsey of any changes to those locations. Service Provider shall implement the policies and procedures set out in this Exhibit for its personnel, equipment, and facilities at the locations where McKinsey's Confidential Information may be stored or processed.

11. Physical Security

The Service Provider shall, at a minimum, implement and maintain the following or similar physical restrictions in the locations where Confidential Information is processed or stored by the Service Provider in the performance of the Services:

a. There will be a "clean desk" policy requiring that Service Provider's employees do not leave exposed any data that may be compromised or be used to access Confidential Information or the Service Provider's IT systems through which the data may be accessed.

b. Building access shall be controlled through a two-factor authentication method.

c. All personnel shall be registered and where appropriate required to carry appropriate identification badges.

12. System Testing and Maintenance

The Service Provider shall, at a minimum, implement and maintain the following system testing and maintenance procedures:

a. The Service Provider shall appropriately maintain its IT systems to protect Confidential Information including without limitation:

i) installing security patches within an appropriate time period:

A. within 30 days for critical security patches for operating systems and applications;

B. within 3 months for other types of patches and updates. ii) update or replace any system that is no longer supported by the vendor no later than 6 months prior to the expiration of the vendor's support program; and

iii) ensure that appropriate security agent and malware protection software is deployed and configured to receive daily updates of patches and virus definitions automatically.

b. The Service Provider shall perform appropriate internal and external assessments of and scans and tests for vulnerabilities in all of its IT systems, applications and infrastructure used to provide the Services at least once per month. The Service Provider shall promptly notify McKinsey if any scan compromises the security, confidentiality, integrity, or availability of Confidential Information. The Service Provider shall promptly remedy all vulnerabilities detected from such assessments within a reasonable period of time in accordance with the risk posed by that vulnerability.

c. The Service Provider shall also maintain an ISO27001, SSAE16 (SOC2 Type II) or similar industry recognized certification to ensure that the security controls in place are appropriate to counter the threats and vulnerabilities relating to the Service Provider's IT systems and applications used to provide the Services. The Service Provider shall notify McKinsey in the event of any lapse or change in the scope of the foregoing certification. The Service Provider shall provide McKinsey with a report detailing the results of that risk assessment (including details of all tests and scans performed on its IT systems) and, if required, a remediation plan to reduce any unacceptable levels of risk in the system. Upon request, the Service Provider shall provide McKinsey with a summary report.

13. Training

The Service Provider shall ensure that all of its personnel (including without limitation all relevant management, employees, contractors and other agents) with access to Confidential Information (or systems through which Confidential Information may be accessed) shall participate in the following training:

a. *Initial Training* - Mandatory training on security practices and safeguards at the time of becoming employed by the Service Provider and setting out disciplinary measures for breaches of the ISMS.

b. *Specific Training for Delivery of Services* - Training upon joining the project team regarding the specific requirements of the Agreement and this Exhibit (such training to be reviewed and agreed upon by the parties).

c. *Ongoing Reinforcement* - Periodic communications (via email, posters, notice boards, and handouts) and refresher training, not less frequently than once annually, detailing the importance of information security and compliance with the Service Provider's ISMS.

14. Personnel Due Diligence

a. *Verification checks.* Carrying out verification checks on permanent staff that will have access to Confidential Information.

b. *Background checks.* Conducting appropriate background checks (where and to the extent permitted by applicable law) and requiring employees, vendors and others with access to the Confidential Information to enter into written confidentiality agreements, in both cases as may be set forth in more detail in the Agreement.

15. Subcontractors

In addition to any other requirements that may be set forth in the Agreement, where the Service Provider is permitted to subcontract the performance of the Services under the Agreement and subcontracts any part of the Services that involves (i) the processing of Confidential Information, (ii) access to systems through which access to Confidential Information may be gained or (iii) the fulfillment of information security functions, the Service Provider shall (a) notify McKinsey of the relevant subcontractor(s) and (b) execute formal agreements with each approved subcontractor that require the subcontractor to implement security controls at least as stringent and comprehensive as those provided in the Agreement and this Exhibit.

16. Close-Out Procedures

Subject to the provisions in the Agreement, on termination or expiry of the Agreement, the Service Provider shall notify McKinsey of the Confidential Information in its control and (in accordance with McKinsey's instructions) promptly return or securely delete such Confidential Information.

17. Incident Response Plan and Contingency Plan

The Data Importer shall document and when appropriate implement the following plans:

a. an incident response plan to address any detected incident that threatens or may threaten the Service Provider's IT systems including an actual or potential breach of the ISMS, unauthorized access, disclosure or use of Confidential Information or any compromise of the security, confidentiality, integrity, or availability of the Service Provider's IT system or Confidential Information, in which the plan shall include without limitation a requirement to:

   i) immediately notify the Service Provider's Security Officer and all other relevant security stakeholders (including McKinsey's security team) of the incident;

   ii) promptly track and respond to such incidents and immediately mitigate any harmful effects; and

   iii) report to McKinsey frequently with information on progress and, as appropriate, with summaries of all forensic investigations and remedial action.

b. unless otherwise addressed in the Agreement, a contingency plan to address incidents that result in damage to the Service Provider's IT systems or to the Confidential Information to ensure that such systems and data are restored within 24 hours, and such plan shall include provisions dealing with data backup and disaster recovery.

The Service Provider shall assess and where appropriate update and improve both plans on at least an annual basis.

18. Security Incidents

In the event that an incident that threatens or may threaten the Service Provider's IT systems, including an actual or potential breach of the ISMS, unauthorized access, disclosure or use of Confidential Information or a compromise of the security, integrity, confidentiality or availability of the Service Provider's IT system or Confidential Information ("Security Incident") is detected:

a. the Service Provider shall notify the following McKinsey's security officer via the contact details below (or such other security personnel and contact details that are provided to the Service Provider from time to time) within 24 hours of the Security Incident being detected:

   McKinsey Global Help Desk Incident Management

   Phone: +1-212-798-0813

   Email: ghd@mckinsey.com

b. the Service Provider will provide to McKinsey's security personnel referred to in Section 19.a above, within 48 hours of the Security Incident being detected, a written report describing the Security Incident and the action taken by the Service Provider in response;

c. where remedial work on the Service Provider's ISMS to prevent the Security Incident reoccurring, the Service Provider shall complete that work within 10 working days (for critical remedial work with high impact on the Service Provider's IT systems and/or the Confidential Information) or within a reasonable period of time (for all other remedial work);

d. the Service Provider shall provide McKinsey's security personnel referred to in Section 18.a above with daily updates of the Service Provider's progress in responding to each detected Security Incident (including any remedial work), if any material information in reporting on the Security Incident has been omitted (including reasons for the delay) and when actions taken to remediate the Security Incident are complete;

e. the Service Provider shall not notify third parties, including authorities, data subjects or clients or customers of McKinsey, without McKinsey's express prior consent, except where such notification is required by law or regulation; and

f. McKinsey shall be entitled to inform public authorities, banks and other financial and credit institutions and individuals about the Security Incident should McKinsey be required by law or regulatory body or otherwise consider it necessary to do so.