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 McKinsey 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. Implementing and complying with a written information security program consistent with established industry standards and including administrative, technical, and physical safeguards appropriate to the nature of McKinsey Data and designed to protect such information from: unauthorized access, destruction, use, modification, or disclosure; unauthorized access to or use that could result in substantial harm or inconvenience to McKinsey, its clients or employees; and any anticipated threats or hazards to the security or integrity of such information;

2. Adopting and implementing reasonable policies and standards related to security;

3. Assigning responsibility for information security management and data protection and to provide to McKinsey contact details of responsible persons of Service Provider;

4. Devoting adequate personnel resources to information security;

5. Carrying out verification checks on permanent staff that will have access to McKinsey Data;

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

7. Conducting training to make employees and others with access to McKinsey Data aware of information security risks and to enhance compliance with its policies and standards related to data protection, as well as requiring such personnel to sign an obligation to keep all McKinsey Data confidential and secure (data secrecy) during their assignment and thereafter;

8. Preventing unauthorized access to the McKinsey Data through the use, as appropriate, of physical and logical (passwords) entry controls, secure areas for data processing, procedures for monitoring the use of data processing facilities, built-in system audit trails, use of secure passwords, network intrusion detection technology, encryption and authentication technology, secure log-on procedures, and virus protection, monitoring compliance with its policies and standards related to data protection on an ongoing basis. In particular, Service Provider has implemented and complies with, as appropriate and without limitation:

    - Physical access control measures to prevent unauthorized access to data processing systems such as entry controls including the legitimization of authorized persons (e.g., access ID cards, card readers, desk officers, alarm systems, motion detectors, burglar alarms, video surveillance and exterior security);

    - Denial-of-use control measures to prevent unauthorized use of data protection systems by technical (keyword/password protection) and organizational (user master record) measures concerning user identification and authentication (e.g., automatically enforced password complexity (*inter alia* special characters, minimum length, regular change of keyword), automatic disabling (e.g., keyword or screensaver password activation) and change requirements, creation of one master user record per user, encoding of data carriers, firewalls);

- Requirements-driven authorization scheme and access rights (including different forms of profiles, roles, transactions and objects), and monitoring and logging of system access to ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that McKinsey Data cannot be read, copied, modified or removed without authorization;

- Data transmission control measures to ensure that McKinsey Data cannot be read, copied, modified or removed without authorization during electronic transmission, transport or storage on data media, and transfer and receipt records. In particular, Service Provider's information security program shall be designed:

  i. To encrypt in storage any data sets in Service Provider's possession that includes sensitive McKinsey Data.

  ii. To ensure that any sensitive McKinsey Data transmitted electronically (other than by facsimile) to a person outside of Service Provider's IT system or transmitted over a wireless network uses encryption to protect the security of the transmission.

  iii. To use adequate measures for any other McKinsey Data (e.g., encryption, encoding/tunnel connection (VPN = Virtual Private Network), electronic signature, logging, transport security).

- Penetration tests conducted on Service Provider's IT systems and application platforms no less frequently than once annually by an independent third-party security firm.

- Data entry control measures to ensure that it is possible to check and establish whether and by whom McKinsey Data has been input into data processing systems, modified, or removed by logging and log evaluation systems;

- In addition to any other requirements that may be set forth in the Agreement, subcontractor supervision measures to ensure that, where the Service Provider is permitted to subcontract under the Agreement and any part of the Services involves (i) the processing of McKinsey Data, (ii) access to systems through which access to McKinsey Data 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.

- Measures to ensure that McKinsey Data is protected from accidental destruction or loss including, as appropriate and without limitation, data backup (mirroring of data), retention and secure destruction policies, secure offsite storage of data sufficient for disaster recovery, uninterrupted power supply, and disaster recovery and emergency programs;

- Measures to ensure that data collected for different purposes can be processed separately including, as appropriate and without limitation, physical or adequate logical separation of client data (e.g., "internal client capability"/purpose limitation, separation of functions as production and test).

- The ability to correct, delete or block the McKinsey Data processed on behalf of McKinsey only in accordance with the instructions of McKinsey.

- Upon the earlier of the termination of the processing activities under the Agreement or McKinsey's demand, the return or secure destruction (as determined by McKinsey) of the McKinsey Data processed in connection with the delivery of the Services under the Agreement.

9. Reporting incidents to McKinsey that threaten or may threaten the Service Provider's IT systems, including any unauthorized access, disclosure or use of McKinsey Data or a compromise of the security, integrity, confidentiality or availability of the Service Provider's IT system or McKinsey Data ("Security Incident") immediately, but in no event longer than within 24 hours of the Security Incident being detected, by notifying:

    McKinsey Global Help Desk Incident Management

    Phone: +1-212-798-0813

    Email: ghd@mckinsey.com

10. Taking such other steps as may be appropriate under the circumstances.