EXHIBIT F

Information Security Requirements for External Workers

1. Service Provider shall ensure that the External Workers comply with the following:

    a) Access the McKinsey or client environment only via Firm-approved IT Resources or mechanisms with appropriate business approvals, and in accordance with the Agreement and this Exhibit.
    b) Data must not be transferred onto portable media devices unless it is a McKinsey or client provided and encrypted USB device.
    c) Do not use third-party web-based applications or file sharing systems for the storage, sharing or processing of McKinsey and client material. Data should only be exchanged via Box.
    d) If source code or any part thereof is reused or shared in a public repository such as GitHub, it must not, in any way, be attributable to McKinsey or client.
    e) Service Provider must report data breaches involving McKinsey and/or client information immediately to its contact at McKinsey.

2. Service Provider agrees and acknowledges that as between the Parties, McKinsey retains ownership of all McKinsey IT Resources. "**IT Resources**" shall include all devices, laptops and other software or hardware provided by McKinsey, and shall be considered McKinsey's Confidential Information. Upon completion of the Services, expiration or termination of the applicable SOW, or upon McKinsey's request, Service Provider shall promptly return to McKinsey all IT Resources (except as otherwise requested by McKinsey in writing).

3. Service Provider shall provide, and shall ensure its External Workers provide, all Services solely through McKinsey's IT Resources, except as otherwise approved by McKinsey in advance in writing. To the extent McKinsey provides such approval for Service Provider's External Workers to use a non-McKinsey IT Resource to provide Services and/or to access certain data or systems, Service Provider shall comply with the following additional requirements:

    a) Have antivirus software installed and capable of detecting and protecting against malicious software and spyware. In addition, antivirus signatures must be configured to update daily and to run full system scans on a periodic basis.
    b) All guest and unauthenticated accounts should be disabled.
    c) If the device is configured to automatically back up, McKinsey and client data must be excluded from the backup.
    d) Have a password policy to enforce complex passwords of at least 12 characters. Passwords should use at least 3 of the 4 complexity requirements: uppercase letters, lowercase letters, numbers, and nonalphanumeric characters.
    e) McKinsey and client data must always be stored in an encrypted format using full-disk encryption.
    f) Local firewall must be enabled and configured to block unknown outgoing and incoming connections by default.
    g) All critical security updates for OS and applications are installed within 10 days (or have auto-install enabled).
    h) Securely delete all McKinsey or client data and provide written confirmation of the same at the conclusion of the project with McKinsey and/or upon McKinsey's request.