The purpose of this policy is to govern the acquisition, usage, and management of wireless Mobile devices for Total Energy Services Inc. and its subsidiaries (collectively "Total") business use by the organization's employees. These devices and associated services are provided by Total In addition, this policy outlines appropriate standards and procedures for accessing Total's networks, systems, databases, servers, and other IT infrastructure via mobile devices.

It is also the purpose of this policy to protect corporate resources and information from the misuse or abuse of Mobile-related technologies that could result in malicious attack from hackers, loss or theft of company data, damage to critical applications, and so on.

Scope

This policy applies to the use of all Total company owned mobile devices or BYOD mobile devices for all corporate uses and locations, including main office, satellite offices, home, field locations, telecommuting sites, pre-approved mobile workers on the road, etc.

Possession and use of a company-owned and supported mobile device or use of a personal device with corporate data is a privilege, not a right. Employment at Total does not ensure eligibility. Any employee requiring the use of a Mobile Device must receive prior approval from his or her manager via an approved business case, application, or other channel stating why the employee needs such technology to fulfill his or her job duties.

Appropriate Use

Any Total employee who connects to the corporate e-mail system, whether internally or externally must ensure that his or her connection and correspondence is secure. Mobile devices and services used to conduct Total business must be used responsibly and ethically.

- Issued mobile devices are for corporate business activities. Casual personal use is permitted, but may be revoked if abused. This includes inappropriate or excessive use of email, web-browsing and applications according to corporate web usage policies. Excessive personal calls, e-mails, or text messaging during the work day, regardless of the device used, can interfere with employee productivity and be distracting to others. Employees should attempt to handle personal matters on non-work time. It is understood that this is required at times but should not result in the bulk of your day unless due to emergency situations of which your manager should be aware.

- No employee shall use personally-owned Mobile devices or services for Total business without the approval of their Manager and the Vice President – Operations of Total. If approved, the personally owned device must be enrolled within Total's mobility management services through the IT department.

- Acquisition of any and all mobility-related technology must be done in accordance with Total's purchasing and procurement procedures as established by Total.

- As the integrity of data on mobile devices is the sole responsibility of the user, and common sense physical security measures should be employed at all times to prevent theft or loss. Users must report loss or theft of a device immediately to their manager and the IT department.

- All mobile users agree to immediately report any incident or suspicion of unauthorized access and/or disclosure of corporate data or resources.

- If a mobile device's native purging features are damaged beyond its ability to ensure that no data remains, or if the device is damaged beyond repair, the device will be destroyed and disposed of in accordance with Total's disposal procedure.

- Total will manage all usage via the centralized Enterprise Mobility Management server. Mobile usage will be monitored to ensure the service is being used appropriately.

- All mobile users agree and understand that usage may also be monitored to record dates, times, duration of access, and so on in order to identify suspicious activity or potential security breaches. If required, users also agree that Total may issue a remote wipe on the device which may make all personal data unavailable.

- Access to all corporate systems and data via a mobile device must be protected by a strong password system that complies with Total's password policy. Passwords should be changed every sixty (60) days.

- Mobile users shall refrain from sending or storing sensitive data on their devices (e.g. personal data, financial data, proprietary data, records about individuals requiring full protection), as per privacy legislation governing Total.

IT Regulation and Authority

This policy governs all Total employees (FTE, PTE), contractors, freelance workers, and others who use mobile technology to access corporate resources for the purpose of conducting Total business and operations. Total reserves the right to revoke mobile access privileges at any time and without notice should it be deemed necessary or desireable to do so.

This policy covers all technological aspects of Mobile device connectivity, including the handhelds themselves, Mobility-related server management software, Mobility-related desktop software, and any other software or hardware deployed to interoperate with Mobile Device technology.

Total's IT department has responsibility for the installation, configuration, and security measures of mobile devices and related technology. If any non-approved device, installation, or technology is discovered, the IT department may remove and/or deactivate it immediately and without notice.

Total reserves the right to deactivate any and all mobile devices, services, e-mail servers, etc. without prior notice to mobile users if any activity or incident occurs that puts corporate resources, data, users, etc. at risk.

This corporate Mobile Device Policy is approved this 15th day of October, 2020.

Brad Macson
Vice President, Operations