SECURITY POLICY

Acceptable Use policy:

The corporation reserves the right to monitor all of the IT resources, telecom and also the network to guard the integrity of all the information systems and computer equipment on the compound.  This is set in place to ensure that the usages of the equipment are in compliance with the acceptable use policy.

ACCEPTABLE USE

* Work related research and the gathering of information.
* Analyzing project related documentation and information.
* Arranging data that is pertinent to job tasks.
* Completing projects and assigned tasks.
* Obtaining data for marketing and commercial reasons.
* Online training/learning

UNACCEPTABLE USE:

* Any illegal activities, gambling or any violations of the copyright laws including the downloading of music and software are absolutely prohibited.
* Personal commercial use and or any profit-making intentions
* Attempts to hack or alter any of the corporations’ systems
* Establishing any unauthorized access to files, folders or databases by the means of using other personnel credentials.
* Broadcasting any derogatory, threatening or prejudice messages.
* Violating system policies
* Sharing sensitive material to unauthorized personal.
* Playing online video games
* Visiting vulgar, disturbing, and adult websites

USER ACCOUNT MANAGEMENT

The corporation employees have the ability to manage and modify certain aspects of their accounts. The Acceptable Use Policy sets the requirements for each employee at the firm.

* Managing your user account
* The ability to change and reset passwords
* The option to check quota for accounts such as emails
* Access rights to the wireless network
* Access to staff logins
* Login to company portal
* Login to the company’s intranet.

HOW I WOULD SET UP A COMPANY VPN FOR REMOTE ACCESS:

* Use Client-based Remote Access software
* Preferably a Multi-protocol setup, (for efficiency with videos and video calls)
* Use OpenVPN protocol for customizability, security layering, and efficiency. (primarily for workstation and data use)
* Use IKEv2 protocol for video meetings and non-sensitive information over mobile access
* For security purposes, integrate 2-factor authentication using standard login password and (preferably) a physical key (USB based cryptographically unique key), with a separate option of using biometrics for those with webcams.