Notes

1. The software product used to achieve the design is **libre office 7.2.5** with an extension of **VRT network equipment 1.2.0**

2. **Include in your design multi-factor authentication to the computer using the Microsoft Authenticator or the Google Authenticator Mobile Apps.**

   I. For a user to activate his multi factor verification he must:
   II. Open a Google Account
   III. In the navigation panel, select security.
   IV. Under "signing into Google," Select 2-Step verification and Get Started.
   V. Follow the on-screen steps.
   VI. After which the user signs in to their google account using his smart phone using, the Gmail app or google app.
   VII. A notification will pop-up for the user to either allow sign-in or block sign-in.

3. **Include a plan for migrating the current local users onto the new system in the shortest possible time.**

   The simplest way to migrate all current local users is to back up and copy their user profile from the old system which includes collecting files and settings from the source computer after which you prepare the destination computer and restore their user profiles.

4. **Design how to setup a Virtual Private Network for remote workers to be able to access the office network.**
   I. In setting up a vpn for remote workers to be able to access the office network.
   II. First, the key VPN components need to be setup (VPN Client, VPN server and VPN router).
   III. After which the VPN client software should be installed, and the user will then log in using his credentials then vpn client automatically connects to the nearest location.
   IV. The user then decides which protocol will be favorable to him which includes improved speed, improved data privacy and security.
   V. Finally, the user must fine-tune the connection which means making sure the VPN settings suit his business needs.

5. **The actual steps required to setup and configure the software to bring it to a usable state.**
   I. ISP will provide internet which will be connected through the vpn to our firewall which also serves as a router.
   II. Our central servers, web server and application server will be assigned static class C IP address which will be connected to a switch which is also assigned a static class C IP, including a wireless router.

III. Now each department computer will be assigned a unique class C IP address just to differentiate them.
IV. Also, all the department computers in each department are connected to a switch which is then connected to the firewall.

6. **Security Checks include:**

i. Installation of antivirus and antimalware which will protect the organizations network from viruses, trojans, ransomware, spyware, worms, and other unauthorized programs planted on the network.
ii. Firewall to control the traffic going in and out of your network through a series of rules and block unauthorized traffic before they breach the internal network.
iii. Data loss protection also helps to protect your data by monitoring the network, so users don't violate the policy you set for sensitive data.
iv. Consistent Software update because delay in update may cause you to miss out on fixes to known security vulnerabilities, putting your data at risk.
v. Other security checks include user account management, software patches, limiting remote access and its policies, making sure employees set a very strong password and finally train your workforce and protect against security threats.