# Network Maintenance Schedule

* All clients within the network must be installed with the business plan of MalwareBytes which offers internet security, configure it to do a threat scan once in every 2 days. A full scan must be done once in every week. The IT Staff should then take the logs, quarantine the issues and advise the user of the client as to how to avoid these issues.
* WireShark must be used by the IT staff at the server room to sniff packets, every week a soft copy of any unrecognized or unauthorized logs must be maintained and inserted into a folder.
* The IT staff must always investigate any suspicious activity within the network with the help of WireShark.
* Metasploit must be used to check for exploits and loopholes in the security of the network once in every month.
* Trace route testing must be used within the network to troubleshoot problems.
* With the help of KerioControl, the firewall must be tested and all rules given for the firewall must be checked every hour.
* Every day it is **COMPULSORY** to make a **complete** backup of the critical information of the server and store them in an external hard disk that must be stored within the server room under lock and key in an anti-fire, anti-shock, waterproof environment, all information stored in this hard disk must be encrypted using AES 128-bit .
* In the event in which the company network has been or is highly probable to be hacked, the IT staff must communicate with me, K.P.I. Shenesh Perera in order to take appropriate measures. However before I arrive, it is recommended that the IT staff has reconfigured IP addresses, temporarily shut down the route from the hacked branch to the other branches.
* In the event that any of the network devices are malfunctioning, per the justification replace the device from the same distributor.
* In the event of a natural disaster, retain the previously mentioned backups and start restoring the server. If the server is damaged, restore the server then restore the data using the backups.
* In the event of a virus/malware infection, immediately do full scans in all clients and temporarily shut down the switch of the infected floor in order to prevent transfer to other floors.
* All rackmounted switches must be placed in air conditioned rooms.
* All network cable connections must be checked once in every month or if there is an event in which the network is not functioning.
* If network cables have to be replaced, use the excess network cables stored per the justification or contact the same distributor and buy in excess to the required length. Store the remnant.
* The server operating system must be updated as soon as there are any updates available **BUT** ensure that a system restore point has been made before updating, in the case of which an update corrupts the system, roll back to the previous restore point.
* The laptops in the accounting department are also vulnerable to the above rules.
* All wifi routers must be set with inbound and outbound rules, and be configured with proxy rules to ensure that employees only surf company websites.

All company employees in both Kandy and Colombo **must** follow the company’s security and privacy policy, the IT staff must ensure that their local branch’s employees follow all security guidelines strictly. Intending to or attempting to damage, harm, disrupt or access the network without authority by employees must be punished severely.