Appendix 4

GUIDELINES ON USE OF COMPUTER FACILITIES

1. These guidelines apply to employees to whom Company computer and communication facilities are made available and to those who use or gain access to the Company computer network. Adherence to these guidelines minimizes the risk of breach of integrity of the Company's computer systems, reduces the likelihood of any legal liability against the Company and employees, and optimizes the use of the Company's resources.

2. Computer and communication facilities are provided to employees for economical, effective and efficient performance of their work/duties.

3. Computers attached to the Company network must not be simultaneously connected to other network.

4. Computers attached to the Company network are installed in accordance with specifications defined by IT Department (ITD). Employees are notpermitted to change any settings without first consulting with ITD. Employees must not attach any device or equipment to the Company network without prior approval of ITD.

5. Employees are responsible for ensuring the physical security of the Company devices under their control.

6. If employees receive an e-mail by mistake they should respect the confidentiality of its contents, delete the e-mail and inform the sender. Employees must not send the e-mail onto the likely intended recipient; this is the responsibility of the original sender.

7. Employees must not install any software without prior approval of ITD.

8. Employees must not make use of Internet chat, instant messaging facilities, data streaming or downloads which are not related to their work.

9. Employees must not divulge their passwords or allow anyone else to use their account at any time. Employees must not use their work password for any other purpose.

10. Employees must ensure their computers are password-locked when left unattended.

11. Users of laptops, personal digital assistants (PDAs), smart phones, etc., must contact ITD to discuss appropriate arrangements for ensuring that security software, such as anti-virus software, system patches and/or personal firewalls, are kept up-to-date.

12. Employees must not allow Company's wireless devices (e.g., Bluetooth devices) to be accessible to other devices without appropriate authorization.

13. All employees must report to ITD actual or suspected security incidents.

14. On leaving the Company employment, employees must return all Company-owned computerand communication equipment and data that have been issued to them. Employees must also return equipment and software licenses upon demand by the Company.

RIJALUDDIN SALLEH
Senior General Manager, Head
Group Compliance & General Services Division