Best Practices for Mobile Phones/ Tabs

1. Do not store any classified / sensitive data (text / video / photograph) in the device.

2. Read vendor privacy policies before downloading apps and app permission should be reviewed closely.

3. Disable installing of third party apps from unknown sources.

4. Avoid use of wallet aggregator apps, which stores / links other e-wallets and bank apps.

5. Auto start, data usage for each App and App permission should be controlled through the security features available.

6. Review the default privacy settings of smart phone apps or services and, if needed, change the settings; e.g. settings about Whether or not to attach location data to images, to social network posts. etc.

7. Relevant anti-virus software should be installed in the smart device and same be updated regularly.

8. Turn off GPS location services when not needed.

9. Turn off/ remove the apps which are not needed.

10. When device is idle, it should get locked and require a password/ pin or swipe pattern. Set the device to lock in relatively short time.

11. Take back-up of data (contacts, personal photos, etc.) on external media.

12. Do not reply or click on link on SMS or messages or photos sent by strangers.

13. There are numerous threats associated with Wi-Fi hotspots. To be safe, avoid logging into accounts, especially financial accounts, when using public wireless networks.