NCC
NIGERIAN
COMMUNICATIONS
COMMISSION

GUIDELINES FOR SECURING MOBILE DEVICES

The following guidelines are intended to help mobile computing device users protect the data the devices contain. These guidelines are easy to implement and can protect users' privacy and data in the event that the device is compromised, lost or stolen.

- Users should label their devices by name and a phone number where they can be reached to make it easy to return if it is lost, even if the battery is dead.
- Configure a passcode to gain access to and use the device. This helps prevent unauthorized individuals from gaining access to your data.
- Set an idle timeout that will automatically lock the phone when not in use. This also helps prevent unauthorized individuals from gaining access to your data.
- Keep all software up to date, including the operating system and installed "Apps". This helps protect the device from attack and compromise.
- Do not "jailbreak" or "root" your device. "Jailbreaking" and "rooting" removes the manufacturer's protection against malware.
- Obtain your apps only from trusted sources such as the *Apple iTunes Store*, Windows Phone App store, Blackberry World, *Google Play*, or the *Amazon App Store for Android or from your manufactures App Store*. This helps you avoid malware which is often distributed via illicit channels.
- Enrol your device in a managed environment. This helps you configure and maintain your security and privacy settings.
- If using an iPhone or Apple device users should enrol their devices in Find My iPhone or an equivalent service for other devices. This will help locate your device should it be lost or stolen.
- If your device supports it, ensure that it encrypts its storage with hardware encryption. In conjunction with a management service or "Find My iPhone," this can allow data to be removed quickly in the event that the device is lost or stolen.

**NEW MEDIA AND INFORMATION SECURITY DEPARTMENT
NIGERIAN COMMUNICATIONS COMMISSION**