MOBILE SECURITY

1. Ensure that the mobile operating system is updated with the latest available updates/patches.

2. Don't root or jailbreak your mobile device. Rooting or Jail breaking process disables many in-built security protections and could leave your device vulnerable to security threats.

3. Keep the Wi-Fi, GPS, Bluetooth, NFC and other sensors disabled on the mobile phones. They may be enabled only when required.

4. Download Apps from official app stores of Google (for android) and apple (for iOS). Do not install apps from untrusted sources unless you are sure about the source of the app.

5. Before downloading an App, check the developer & popularity of the app and read the user reviews.

6. Observe caution before downloading any apps which has a bad reputation or less user base etc.

7. While participating in any sensitive discussions switch-off the mobile phone or leave the mobile in a secured area outside the discussion room.

8. Don't accept any unknown request for Bluetooth pairing or file sharing.

9. Before installing an App, carefully read and understand the device permissions required by the App along with the purpose of each permission.

10. ln case of any disparity between the permissions requested and the functionality provided by an app, users to be advised not to install the App (Ex: A calculator app requesting GPS and Bluetooth permission)

11. Note down the unique 1S-digit lMEl number of the mobile device and keep it offline. lt can be useful for reporting in case of physical loss of mobile device.

12. Use auto lock to automatically lock the phone or keypad lock, protected by pass code/ security patterns, to restrict access to your mobile phone.

13. Use the feature of Mobile Tracking which automatically sends messages to two preselected phone numbers of your choice which could help if the mobile phone is lost/ stolen.

14. Take regular offline backup of your phone and external / internal memory card.

15. Before transferring the data to Mobile from computer, the data should be scanned with Antivirus having the latest updates.

16. Observe caution while opening any links shared through SMS or social media etc., where the links are preceded by exciting offers/discounts etc., or may claim to provide details about any latest news. Such links may lead to a phishing/malware webpage/app, which could compromise your device.

17. Report lost or stolen devices immediately to the nearest Police Station and concerned service provider.

18. Disable automatic downloads in your phone.

19. Always keep an updated antivirus security solution installed.