Subject: **Advisory - Prevention Against Vulnerabilities of iPhone (Advisory No 47)**

1. Context. **Security researchers** have found **critical vulnerabilities** in **apple** products that can **leak sensitive** information to third parties. These **weaknesses** have **previously** impacted **android** products only and now they can also affect **apple** devices.

2. **Risk associated with use of iPhones**

a. Attackers **exploit** weaknesses related to **iPhone** that can come from **Bluetooth, mobile device management (MDM), meltdown** and **specter** etc.

b. **Apple's online** service, **iCloud,** allows seamless access, management, editing and sharing from **iPhone, iPad,** and **Mac.** However, there is a **risk** associated with **data leakage,** as users don't have any **control over data.**

3. **Mitigation Measures.** For **safe usage of iPhone** following **best practices** are recommended:-

a. **iPhone Configuration**

(1) Always update **firmware (i0S)** to latest **version.**

(2) **Turn off,** ask to join networks and **auto-join** for all networks.

(3) Turn off **Location Services** unless necessary for **specific apps.**

(4) Always enable and set difficult **passcode/ PIN** to **unlock** the iPhone.

(5) Set **auto-lock** timeout to a period of **5 minutes** or less.

(6) Disable **SMS preview** when the **iPhone is locked.**

(7) Enable **erase data** upon excessive **password failures.**

(8) **Delete** any **widgets** that displays **personal** info.

(9) **Disable tracking:** Head to Settings > Privacy > Location Services > System Services and turn off Frequent Locations.

(10) **Turn off** contact, photo, email, or calendar, location access in apps that don't need it.

(11) Turn on **two-factor authentication.**

(12) Enable **Fraud** warning in **safari browser.**

b. **Safe Usage of iPhone**

(1) Turn **on airplane mode** when you do not need the **phone, GPS, radio, Wi-Fi,** or **Bluetooth.**

(2) Only **turn on WiFi & Bluetooth** when you need to connect to a Wi-Fi and Bluetooth network.

(3) Use the **cell carrier's** network instead of an **insecure Wi-Fi** network.

(4) Use public **WiFi** .**hotspots** with **caution** and configure the smartphone so that it **does not** connect **automatically.** Use only **trusted networks** for sensitive matters, e.g., embanking/ commerce, and emailing.

(5) Never **jailbreak** your **iPhone.**

(6) **Erase** all data before **selling** or **recycling** your iPhone.

(7) **Check reputation** before installing or using new Smartphone apps or services.

(8) **Immediately change** all saved **passwords** (Google, Facebook, twitter etc.) on the **iPhone** in case phone is **lost** or **stolen.**

4. **Recommendations.**

a. Strictly follow all **mitigation measures** discussed at **Para 3** for **safe** and **secure** usage of iPhone.

b. Remove all **unnecessary apps** installed from **smart phone** and install only **limited apps** from **apple play store.**