# Code of Practice on the Operation and Management of Internet of Things Devices

## Introduction

Pursuant to General Condition 5.1 of the Unified Carrier Licence ("UCL") and the Wireless Internet of Things ("WIoT") Licence, fixed and mobile network operators licensed under the UCL and service providers licensed under the WIoT Licence, in providing communications services and platforms for Internet of Things ("IoT") devices, (hereinafter collectively referred as "IoT service providers") are required to provide a good, efficient and continuous service in a manner satisfactory to the Communications Authority ("CA"). Pursuant to Special Conditions 1.2(a) and (c) of the UCL and the WIoT Licence, the CA may issue guidelines for the purpose of providing practical guidance to the licensees in respect of the provision of a satisfactory service and to ensure the protection and promotion of the interests of consumers of telecommunications goods and services.

2. IoT devices are typically used for automated machine-to-machine type applications. With the development of new wireless technologies such as the fifth generation ("5G") mobile technologies and new smart city applications, it is expected that there will be a massive number of IoT devices connecting to the public telecommunications networks in the coming years, some of which may also support sophisticated and even mission critical applications such as autonomous vehicles. The proliferation of IoT devices deployed for a wide range of applications and the collection/processing of a vast amount of data using IoT devices will bring new challenges for data protection and security. There is thus a need to ensure proper operation and management of these IoT devices which will connect to the public telecommunications networks to safeguard the interests of both the consumers and the business sectors in the IoT era.

3. To ensure the provision of satisfactory service by IoT service providers, strengthen consumer protection and enhance user confidence

in using IoT devices connecting to public telecommunications networks, IoT service providers should observe the best practices as set out in this Code of Practice ("CoP") on a voluntary basis. For non-telecommunications licensees such as device manufacturers, vendors, application developers who may supply and deploy IoT devices in the telecommunications and other business sectors (e.g. personal, leisure, household, transport, medical, financial sectors), this CoP can also serve as a reference to assist these sectors in formulating suitable requirements and practices regarding the operation and management of IoT devices/services.

## Challenges Identified

4. In the IoT era, it is necessary to resolve the security challenges inherent to its growth. These challenges are –

(a) **Privacy**: reducing the potential for harm to individual end-users;

(b) **Identity**: authenticating IoT devices, services and end-user operating the IoT devices;

(c) **Security**: ensuring system integrity of IoT devices to effectively prevent and sustain cyber attacks (e.g. IoT devices being exploited for launching a large-scale cyber attack, such as the Distributed Denial of Service attack) whilst associated data can be verified, tracked and monitored; and

(d) **Availability**: ensuring stable connectivity between IoT devices and IoT services.

## Best Practices to Adopt

5. A number of industry bodies and international organisations have developed best practices in respect of the operation and management

of IoT devices (some of which are set out at **Appendix**). IoT service providers should draw reference from these best practices in developing their own operation and management mechanism. The practices listed below are of particular importance; and IoT service providers should adopt these practices as far as possible –

(a) only IoT devices provided by manufacturers/vendors which implement appropriate security policies and resilient measures[1] should be deployed. Suitable testing should also be conducted to verify individual functions and features of such devices before deployment;

(b) unique usernames and strong passwords should be adopted for IoT devices. Where applicable, alternative methods of authenticating users including multi-factor authentication (e.g. using an electronic token in addition to a username and password) and identity management technology (e.g. SIM card) should be adopted. IoT devices with hard-coded usernames and passwords in the device software should not be adopted;

(c) users should be provided with a point of contact to report security issues. Disclosed vulnerabilities should be acted on as soon as practicable to minimise the adverse impact brought about by the security issues identified. Where applicable, such information should be shared with relevant manufacturers and vendors of the IoT devices;

(d) software of the IoT devices should be updated in a timely manner and should not impact on the functions of the devices. The need for each update should be made clear to users and the update should be easy to implement. IoT device should be replaced if the software is no longer updatable;

[1] For example, IoT devices would be able to run independently, securely and safely with basic functions even when there is a failure of IoT platform or loss of network connection. When the IoT platform or network connections is recovered, the IoT devices should be able to resume full functions.

(e) sensitive data (e.g. personal data, device identifiers, usernames, passwords) should be stored securely (ideally with encryption) in the IoT devices to prevent unauthorised access and modification. Such data should also be end-to-end encrypted before transmission in networks. Where applicable, security mechanisms (such as anti-virus and anti-malware protection, network firewall and access control list) should be put in place to protect the IoT devices from attacks;

(f) personal data should be protected in accordance with the Personal Data (Privacy) Ordinance. Users should be informed as to how their data will be used for each IoT device. Personal data should be permanently and easily erased from IoT devices when there is a transfer of ownership or disposal of IoT devices;

(g) the security and privacy settings of IoT devices should, as far as possible, be configured to the highest level with the minimum set of rights provided to users as necessary for operating IoT devices. Only essential network interfaces should be open for access. Other components of the IoT devices (e.g. camera, loud speaker, and microphone) should be disabled except in use;

(h) the integrity of the software of IoT devices should be verified. If an unauthorised change to software is detected, the connection of IoT devices to network should be disabled and users should be alerted;

(i) formats, types and values of data which are input by users, collected by IoT devices from the environment or transmitted in networks should be validated where applicable and should be monitored for identification of any anomalies (e.g. unscheduled transmission of data). If any anomalies are identified, appropriate mitigating measures should be taken; and

(j) users should be provided with adequate guidance on installation, configuration and use of IoT devices. Users should also be encouraged to follow the best practices at **Annex A**.

## Risk Assessment

6. The operation and management of IoT devices is an on-going process. IoT service providers should regularly conduct assessment on potential risks relevant to their daily operation and management of IoT devices. Key steps in conducting risk assessment process are set out at **Annex B**.

## Application and Update of the CoP

7. This CoP does not replace or substitute the requirement for the operation and management of IoT devices under any agreement made between the IoT service providers and their customers.

8. The CA may review and update this CoP from time to time taking into account technology and market developments, as well as the telecommunications policy.

**Communications Authority**
**June 2019**

**Annex A**

## Best Practices for Users of IoT Devices

Users of IoT devices are encouraged to follow the best practices listed below –

(a) understand the product before purchase;

(b) check the reputation of the manufacturer and find out if it has been involved in any illegal behaviours. Avoid using IoT devices that do not have inquiry/support service or when the original manufacturer/vendor of the IoT devices no longer exists;

(c) set a unique username and strong password for each device, never divulge the username / password to other people, and change the password regularly;

(d) adjust the security and privacy settings to higher levels than default factory settings before using the devices;

(e) perform regular security update of the software of IoT devices. Do not use IoT devices if the software is no longer updatable;

(f) avoid using IoT devices that transmit personal data as far as possible. Disable functions and turn off such devices if they are not in use, and erase all information and personal data before disposing of the IoT devices; and

(g) enquire about the network condition for IoT devices if anything unusual is observed.

**Annex B**

## Key steps in conducting Risk Assessment for IoT devices

IoT service providers should formulate their own risk assessment procedures with reference to relevant frameworks and models issued by industry organisations and standards bodies. They should also conduct regular risk assessment regarding the operation and management of IoT devices adopted, taking into account the following key steps –

(a) identify the IoT devices that need to be protected;

(b) identify the vulnerabilities of IoT devices operated;

(c) identify the types and causes of issues and incidents that can pose ineffective operation or management of IoT devices;

(d) identify and understand the consequences (e.g. monetary loss, cyber security threat, harm to health, pollution and safety impact) and possibilities of ineffective operation and management of IoT devices;

(e) study and implement mitigating measures to minimise the negative effect of these consequences;

(f) implement measures to eliminate potential vulnerabilities of IoT devices;

(g) estimate resources (e.g. financial, human and technical resources) needed for incident responses, monitoring, and remediation; and

(h) maintain proper documentation on security risk assessment for IoT devices.

## Appendix

## Reference Documents

"Code of Practice for Consumer IoT Security", Department for Digital, Culture, Media & Sport, United Kingdom, October 2018

"IoT Security Guidelines Overview Document" Version 2.1, GSM Association, 31 March 2019

"IoT Security Guidelines for IoT Service Ecosystem" Version 2.1, GSM Association, 31 March 2019

"IoT Security Guidelines for IoT Endpoint Ecosystem" Version 2.1, GSM Association, 31 March 2019

"IoT Security Guidelines for Network Operators" Version 2.1, GSM Association, 31 March 2019

"IoT Security Compliance Framework" Release 2, IoT Security Foundation, December 2018

"IoT Security Guidelines" Version 1.0, IoT Acceleration Consortium, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry, Japan, July 2016

"Enterprise IoT Security Checklist", Online Trust Alliance, Internet Society, United States, 17 April 2018

*****