For Discussion on
19 December 2022

TRAAC Paper No. 4/2022

Telecommunications Regulatory Affairs Advisory Committee

Proposed Update of the "Security Guidelines for Next Generation Networks" and "Code of Practice on the Operation and Management of Internet of Things Devices"

PURPOSE

This paper seeks Members' views on the proposal to update the existing "Security Guidelines for Next Generation Networks" ("NGN Guidelines")[1] and "Code of Practice on the Operation and Management of Internet of Things Devices" ("CoP for IoT devices")[2] by incorporating a new compliance checklist for regular health check by relevant telecommunications operators.

BACKGROUND

2. Telecommunications licensees are required under General Condition ("GC") 5.1 of their Unified Carrier Licence ("UCL"), Services-based Operator Licence ("SBO Licence") or Wireless Internet of Things ("WIoT") Licence to provide a good, efficient and continuous service in a manner to the satisfaction of the Communications Authority ("CA"). Pursuant to Special Conditions ("SCs") 1.2(a), (c) and (e) of the UCL and the WIoT Licence and SCs 12.1(a), (c) and (d) of the SBO Licence, the CA may issue code of practice or guidelines for the purpose of providing practical guidance to the licensees in respect of the provision of satisfactory service, the protection and promotion of the interests of consumers of telecommunications goods and services, and correct, efficient and reliable operation of telecommunications.

[1] A copy of the document is available at https://www.coms-auth.hk/filemanager/statement/en/upload/512/gn082019.pdf.

[2] A copy of the document is available at https://www.coms-auth.hk/filemanager/statement/en/upload/511/cop-iot_e.pdf.

3. The NGN Guidelines were first issued in 2010 to provide practical guidance to facility-based operators which operate NGNs and services-based operators which provide services with the use of NGN provided by others on the provision of security measures for the integrity and proper operation of NGNs as well as protection of data and the users' proper use of the telecommunications services. In 2019, in the light of the development of the fifth generation ("5G") mobile and new emerging technologies including network slicing, network functions virtualisation, software defined networking and edge computing and the increasing proliferation of Internet of Things ("IoT") devices deployed for a wide range of applications including mission-critical services, OFCA, having consulted the TRAAC (vide TRAAC Papers No. 2/2019 and 3/2019)[3] and the industry, updated the NGN Guidelines and issued the CoP for IoT devices with a view to ensuring that these 5G, newer generations of Internet Protocol ("IP") and IoT networks/applications will continue to be protected against new security threats.

THE NEED FOR UPDATE

4. The launch of 5G commercial services of Hong Kong since 2020 has not only brought consumers with a variety of high-speed mobile services with increased capacity and lower latency, but also enabled various industry sectors to have a greater capability and flexibility to deploy IoT devices for new applications, improve their operation efficiency and provide consumers with better service quality and new user experience. These networks, services and applications are a critical part of the information infrastructure in Hong Kong and are essential for the normal functioning of the society and economy. If the continuous, reliable and secure operation of them is adversely affected by malicious attacks or other disruptions, this may cause serious harm to economic activities, public services, people's livelihood, and even national security.

[3] Copies of relevant TRAAC papers are available at https://www.ofca.gov.hk/en/about_us/advisory_committees/TRAAC/papers/index.html.

5. With a view to enhancing the security and reliability of Hong Kong's telecommunications networks, services and applications and further strengthening OFCA's regulatory oversight and effective monitoring, OFCA proposes relevant updates to the NGN Guidelines and CoP for IoT devices whereby operators should, on an annual basis, conduct regular health check and report their status of compliance with the relevant measures and best practices set out in the NGN Guidelines and CoP for IoT devices, as the case may be. Opportunity is also taken to make other minor updates (e.g. format of reporting on security incident) as appropriate.

THE PROPOSAL

Regular health check and submission of compliance checklist

6. It is proposed that the NGN Guidelines and CoP for IoT devices should be updated with a new compliance checklist requirement under which relevant NGN operators and IoT service providers should conduct regular health check and complete, on an annual basis, a checklist about their compliance with the measures and best practices set out in these documents. The completed checklist together with relevant supplementary information and supporting documents (if any) should be submitted to OFCA on an annual basis within a specified timeframe. Where requested by OFCA, relevant NGN operators and IoT service providers should provide a more detailed account of their progress of compliance with specific measure or best practice. Draft revisions to the NGN Guidelines and CoP for IoT devices, together with other relevant updates and textual amendments, are at **Enclosures A and B** respectively.

7. OFCA encourages all NGN operators and IoT service providers, in particular local fixed and mobile network operators, to pledge compliance with the NGN Guidelines and CoP for IoT devices, as appropriate. In recognition of operators for their commitment to compliance with the relevant security measures and best practices for reliable and secure operation of networks/services, OFCA will publish a summary highlighting those operators which have conducted the annual health check and confirmed the overall compliance with the associated security requirements on OFCA's

thematic webpage for information of the public.

Submission of NGN development status

8. From time to time, OFCA is requested by the International Telecommunication Union ("ITU") to submit regular returns on telecommunications development in Hong Kong including NGN development status. With a view to facilitating effective monitoring of relevant operators' NGN development status by OFCA and ensuring that the information provided to ITU would accurately reflect Hong Kong's position, OFCA proposes to take this opportunity to incorporate in the revised NGN Guidelines the requirement of submission of NGN development status by relevant operators to OFCA on an annual basis.

VIEWS SOUGHT

9. Members are invited to give their views and comments on the proposal given in this paper.

NEXT STEP

10. Taking into account the feedbacks from the industry, OFCA will finalise the documents and make recommendation on the matter to the CA for approval.

Office of the Communications Authority
December 2022

Enclosure A

GN-~~8~~X/2023~~19~~

Security Guidelines for

Next Generation Networks

Office of the Communications Authority

Issue ~~3~~4
~~June 2019~~XXX 2023

Amendment History

Item	Issue No.	Issue Date	Paragraph/Section	Description
1	2	21.04.2017	Whole document	(i) Editorial changes to rename OFTA to OFCA; (ii) update OFCA's contact information.
2	3	25.06.2019	Whole document	Inclusion of security measures applicable to networks based on the fifth generation mobile technologies.
3	4	DD.MM.2023	Whole document	Inclusion of a template of status report on NGN development and a compliance checklist against security measures.

FOREWORD

In Hong Kong, public telecommunications operators (hereinafter referred to as “operators”) have established next generation networks (“NGNs”) or are in the process of replacing their traditional service platform with NGNs for the provision of public telecommunications services. NGN usually refers to a platform that has the capability to carry voice, data and video information by using one single service platform based on the Internet Protocol (“IP”)[1].

2. The technologies underpinning NGNs have been evolving over time. The advent of the fifth generation mobile (“5G”) era and the new emerging technologies such as network slicing, network functions virtualisation (“NFV”), software-defined networking (“SDN”) and edge computing not only unveil a new chapter of network evolution, but also open massive opportunities of new telecommunications services and smart city applications, such as enhanced mobile broadband, massive machine-type communications (i.e. Internet of Things in a massive scale), and ultra-reliable and low-latency communications. It enables operators to have greater capability and flexibility to introduce innovative services which will provide consumers with new user experience. NGNs have become a critical part of Hong Kong’s telecommunications infrastructure supporting a large number of customers and are essential for the normal functioning of the society and economy.

3. While enjoying the benefits, operators and consumers may face new security issues brought about by NGNs. As the architecture of NGN is moving towards an open platform that runs everything over IP technologies, it may undermine the integrity and security of network or increase the chance of intrusion. An NGN without proper security measures in place would be highly vulnerable to malicious attacks and pose security threats to its users. If the continuous, reliable and secure operation of NGNs which form part of Hong Kong’s critical information infrastructure is adversely affected by malicious attacks or other disruptions, this may cause serious harm to economic activities, public services, people’s livelihood, and even national security.

[1] For the purpose of this document, the NGN definition introduced by the Telecommunication Standardization Sector of International Telecommunication Union (“ITU-T”) is adopted.

4. This document provides practical guidance on the provision of security measures for the integrity and proper operation of NGNs as well as protection of data and the users' proper use of the telecommunications services. It should be observed by all operators which operate NGNs (facility based operators) ~~or~~ and provide services with the use of NGN provided by others (services-based operators). To safeguard telecommunications network security, operators should conduct regular health check by completing a checklist about their compliance with the relevant security and user protection measures set out in this document, and report their status to the Office of the Communications Authority ("OFCA") on an annual basis. In recognition of operators for their commitment to compliance with the relevant security measures and best practices for reliable and secure operation of networks/services, OFCA will publish a summary highlighting those operators which have conducted the annual health check and confirmed the overall compliance with the associated security requirements on OFCA's thematic webpage for information of the public.

5. To promote user awareness on the security of using the public telecommunications services, operators should from time to time provide updated information to their subscribers about the security vulnerabilities and the capability of their NGNs to manage related risks.

6. In addition to security measures, operators should report any security incidents/violations and their NGN development status in accordance with the procedures set out in this document.

7. For enquiry regarding this document or related issues, please contact ~~–~~

Office of the Communications Authority
29/F., Wu Chung House,
213 Queen's Road East,
Wanchai, Hong Kong
(Attn.: Principal Regulatory Affairs Manager (Regulatory 11))

Telephone no.: 2961 6628

Fax no.:	2803 5112
E-mail:	net_security@ofca.gov.hk

SECTION 1: GENERAL PRINCIPLES

1.1 Operators should take into account the following security objectives, namely confidentiality, integrity, and availability, when building their network and providing their services –

- **Confidentiality** refers to the protection of network and user data from unauthorised access, viewing, diversion or interception;

- **Integrity** refers to the protection of network and user data from unauthorised modification, deletion, creation or replication;

- **Availability** refers to the network and service provisioning to minimise downtime due to security attacks by hackers, if any.

1.2 These objectives provide a foundation upon which a more consistent and structured approach to the design, development, and implementation of network security capabilities can be constructed. The security measures for fulfilling these objectives should not solely focus on technical controls. Consideration on non-technical issues, such as policy and operational procedures, should also be taken.

1.3 While providing adequate levels of protection, the security measures should allow certain flexibility in order to accommodate the rapid change of the telecommunications environment.

SECTION 2: SECURITY FRAMEWORK

2.1 A comprehensive protection of the NGN shall include measures from different perspectives including appropriate risk assessment measures[2] which can effectively counter all possible threats and attacks that may happen in the network.

2.2 A threat is a potential violation of security. Threats may be accidental or intentional, and may be active or passive. An accidental threat is one with no premeditated intent, such as system or software malfunction, or physical failure. An intentional threat is one that is realised by someone committing a deliberate act. When an intentional threat is realised, it is called an attack. An attack may take many forms and may even be premeditated. For example, in the case of an advanced persistent threat, the malware may reside in the target system/network for a few months prior to the launch of the actual attack. Threats associated with NGNs may be classified into (i) destruction, (ii) corruption, (iii) removal, (iv) disclosure, and (v) interruption. Illustration of these security threats is at **Annex 1**.

2.3 To safeguard NGNs against malicious attacks, a set of security measures should be put in place. These measures should address particular aspects of the network security from different dimensions, which may include (i) access control, (ii) authentication, (iii) non-repudiation, (iv) data confidentiality, (v) communication security, (vi) data integrity, (vii) availability, and (viii) privacy. These dimensions represent the classes of actions which can be employed to combat the security threats and attacks. Details of these security dimensions are at **Annex 2**.

2.4 Apart from protecting the operator’s network, user protection and awareness are also critical elements in network security. Operators should provide sufficient measures to protect the users’ proper use of their network services and to promote users’ awareness of potential threats. The ultimate goal is to enable users to adopt appropriate measures available to them in accessing to NGN services.

[2] For example, a Threat Vulnerability Risk Assessment ~~(TVRA)~~ helps identify security threats and vulnerabilities so that measures can be implemented to manage and mitigate perceivable risks.

2.5 To ensure that a security incident/violation can be tackled and managed in a controlled manner, an effective reporting mechanism is required so that the Government and the relevant parties can be kept well informed of the latest development and the impact of the incident/violation. This would enable the Government and relevant parties to take appropriate action/coordination to safeguard the overall interest of the community.

2.6 In addition to the above security considerations, operators should be mindful that any security measures introduced should not deter authorised users from accessing the telecommunications services. Introduction of such measures should strike a reasonable balance between security and user convenience.

SECTION 3: SECURITY MEASURES

3.1 Security measures can be classified into the following three categories, namely management measures, operational measures, and technical measures. The security measures listed below are not exhaustive. Operators should implement other relevant measures to fulfil the principles as set out in Section 1.

Management Measures

3.2 Operators should take into account the following measures when formulating policies for the proper management of their networks and the provision of network services ~~–~~–

(a) implement security policies and measures for the network and review the security aspects regularly in order to cope with the latest technological and business developments;

(b) develop a set of in-house procedures on incident response and remedy, and update the procedures with regard to new potential security threats;

(c) assign clear responsibility to each of the personnel involved in relation to network security under supervision with appropriate access control, real-time monitoring/detection and audit trail systems in place. Assignment of a designated team and contact person for the overall coordination on the incident reporting and handling of significant security incident as specified in ~~s~~Section 5 should also be considered;

(d) implement effective information dissemination mechanism to ensure that network security information, including the security policies, procedures, incident reporting, can be effectively delivered;

(e) perform security risk assessments regularly to fully explore the security posture of the network;

(f) perform independent security audit to verify the compliance of the security posture of the network with the security policy.

Staff in the same organisation who are not involved in network operation can also act as the independent auditor;

(g) implement business continuity plan if the network supports the operator's critical business activities;

(h) implement adequate security control on external consultants, contractors and temporary staff for their access to the network infrastructure; and

(i) ensure that proper security process is in place to manage projects/services which are outsourced.

Operational Measures

3.3 Operators should take into account the following measures in the daily operation of their networks –~~-~~

(a) ensure that updated operational and procedural manuals are available for relevant staff to access and to follow. When a security incident/violation is detected, they should be handled in a controlled manner in accordance with a pre-defined plan to minimise potential damage and to restore to the normal security level;

(b) ensure that all factory default parameters of network equipment or software entities, including login name, administration passwords, IP address range to be allocated to network equipment are properly configured;

(c) ensure that strong security measures[3] are in place for any remote or onsite administration of the network equipment or software entities;

(d) ensure that each platform and device in the network is uniquely identifiable;

(e) ensure that public domain software and freeware is fully tested and verified before putting it to use;

[3] Examples of strong security measures are unique usernames and strong passwords, multi-factor authentication, biometrics and identity management technology, etc. Hard-coded usernames and passwords should not be used.

(f) ensure that proper counter-checking mechanism is in place to guard against any mis-configuration;

(g) maintain the firmware of the network components up-to-date as far as possible;

(h) define and implement an appropriate security right for change control and patch management mechanism for the proper update of network configuration and function, policy settings, security patches and software applications;

(i) review from time to time the validity of encryption keys and renew the keys prior to their expiry;

(j) keep proper documentation on network architecture and inventory records (including firmware and patch version information) of the network components;

(k) keep record of the geographical locations of the physical hardware equipment;

(l) keep record of configuration change logs, access logs and event logs in a secure manner which cannot be modified or fabricated, for a reasonable period of time;

(m) carry out regular system/application/data backup and housekeeping such as removal of unused accounts or services;

(n) select proper location for housing the network equipment so that it is well protected against fire, water flood, etc.;

(o) implement physical security controls to safeguard any unauthorised access and modifications to the hardware, software and network facilities by any unauthorised parties;

(p) ensure that sufficient and uninterruptible power supply and air conditioning/ventilation are available to the network facilities;

(q) implement appropriate security measures to prevent the disclosure of system details of the network;

(r) develop procedures for immediate disabling of any connections of confirmed improper usage;

(s) prevent the security issues occurred in own network from propagation to other networks and manage threats introduced by communications technologies (including NFV and~~,~~ SDN), edge connected devices and other users' devices;

(t) ensure that customer and secured network information is properly erased and unrecoverable before disposal; and

(u) ensure that copyright law restrictions are respected at all times. Only approved software and hardware with proper licences are allowed to be set up and installed following the corresponding licensing agreements and procedures.

Technical Measures

3.4 Operators should implement the following technical measures to protect their networks –~~-~~

(a) design and build the network with infrastructure and facilities which prevent single point of failure, at the core network and, as far as possible, at the edge network connecting to the user's device through an appropriate combination of resilience, redundancy, restoration and repair;

(b) separate the service networks from the operator's corporate networks and adopt network segmentation in the internal network;

(c) assign unique login name and strong password with automatic logout after inactivity for both operational and test systems to reduce the risk of accidental log-on and other errors;

(d) provide a secure location in network platform to store keys for encryption and authentication processes;

(e) implement a standardised random number generation function, and provide source of random data and encryption function which are external to the virtual environment;

(f) provide secured boot feature which validates integrity of firmware / operating system / software entities before execution;

(g) implement authentication and integrity check mechanism between network elements through dedicated hardware module;

(h) make the best effort to avoid conducting development and testing activities in the production environment;

(i) deploy a management platform with network management tools and procedures to ensure controls are consistently applied and services are optimised;

(j) deploy trustworthy anti-virus and anti-spyware systems to help stop any wide spreading of virus, worms, and malicious code through the networks. The definitions should be up-to-date as far as possible;

(k) deploy intrusion detection system ("IDS"), intrusion prevention system ("IPS") or alike to detect the inbound and outbound network traffic as well as detect and log any suspicious activities and network attacks, in particular to block those attacks originated from the associated devices or network elements within their networks;

(l) perform protection according to confidentiality and integrity security objectives for data transmission through network elements;

(m) isolate data logically and/or physically, where appropriate, if they are used by different virtual operators;

(n) implement a secure data storage with access control and authentication mechanisms which prevent any tampering, leakage, unauthorised access or transfer of data. Security level for data being stored and processed at the edge of the network should not be weaker than that for the same data at the core of the network;

(o) implement real-time monitoring system or alike to monitor relevant security activities and resource usage, and examine monitoring records on a regular basis;

(p) execute regular system backup and store the backup data in a secured location;

(q) implement secure authentication methodology and authorisation control to ensure that only authorised staff/users/hosts/devices can access to the network and the services which they subscribe;

(r) implement appropriate separation between network slices when they communicate with users' devices configured with different levels of privileges. Resources and data storage of different network slices should be isolated so that the resource availability and data security of one network slice would not be affected by any other slices;

(s) implement firewalls or alike to protect the networks and prevent the security issues occurring in the network from affecting the users; and

(t) disable unnecessary services embedded in the network elements and close unnecessary interfaces and application programing interfaces of the network platform.

SECTION 4: USER PROTECTION

4.1 Operators should protect the users' proper use of the network services and implement the following measures to safeguard their interests –~~-~~

(a) ensure that customers' information is collected and used in a proper way and in compliance with the Personal Data (Privacy) Ordinance;

(b) implement secure network connectivity to protect the wireline and wireless communications between end-devices and the service networks, including but not limited to the prevention of eavesdropping and altering of the communications content;

(c) employ secured connection such as Secure Sockets Layer ("SSL") when users are asked to input their own account and password in order to ensure the confidentiality of user data;

(d) allow users to establish their own virtual private network ("VPN") connections;

(e) inform users about the proper use of the network services and their responsibilities;

(f) inform and advise their customers from time to time of the risks associated with the network services which the customers subscribe to;

(g) provide prompt information and advice to the customers on security incidents/violations or outages that may affect their network services, and provide a point of contact to users for reporting any security vulnerability; and

(h) provide recommendations to the customers for accessing their networks and inform the customers about the availability of the security measures implemented. A set of recommended "User Best Practice" is at **Annex 3**. Operators are also encouraged to make reference to the Government's one-stop information security portal (https://www.infosec.gov.hk) to obtain the updated user best practices.

SECTION 5: INCIDENT REPORTING

5.1 Telecommunications facility is one of the essential facilities supporting the economy and people's activities in Hong Kong. The outbreak of security incident/violation can result in the degradation or outage of telecommunications services. It is the operators' responsibility to inform the Government of the occurrence of any severe security incident/violation and to provide accurate update of the latest development so that the Government can carry out necessary coordination and arrangement to minimise the impact of the incident/violation to the community.

5.2 If there is an outbreak of security incident/violation which meets any of the triggering events specified below –

(a) a security incident/violation which lasts for more than 30 minutes and results in degradation of service or failure of network component that would affect 10 000 users or more;

(b) a sustained malicious attack experienced by a network element including any tampering/leakage/unauthorised access/transfer of data, interference or damage of critical network facilities/assets/systems/equipment for more than 24 hours; or

(c) a severe security incident/violation which has been confirmed by the overseas counterpart and will likely affect the network service in Hong Kong.

The operator concerned should report the case to ~~the Office of the Communications Authority ("~~OFCA~~")~~ in accordance with the following reporting timeframe –

Reporting Timeframe

Initial Reporting	**Restoration of Service**
The operator concerned should report the security incident/violation to OFCA within one hour after a triggering event for reporting the incident/violation is met	The operator concerned should report to OFCA within two hours after security incident/violation has been resolved

5.3 OFCA will assess the impact of the incident/violation on the territory and determine whether public alert is warranted.

Information to be provided by the operator when reporting a security incident/violation

5.4 When reporting a security incident/violation (which may or may not lead to outage of networks, systems or services) to OFCA, the operator concerned should provide OFCA with the following information, whenever possible ~~-~~

(a) full ~~N~~name of the operator;
(b) ~~D~~description of the incident/violation;
(c) ~~D~~date and time of onset of the incident/violation;
(d) ~~T~~types and estimated number of customers/end-users affected;
(e) ~~A~~affected area(s);
(f) ~~A~~actions taken; and
(g) ~~C~~contact information: ~~(~~name of contact person~~,~~ as well as the person’s fixed and mobile Hong Kong telephone numbers, and email address~~)~~.

5.5. The operator concerned should keep relevant data, including event log and access log, to the extent technically feasible and practicable for the purpose of investigating any security incident/violation including identifying the source of the attack, taking remedial measures and preventing recurrence of similar incidents/violation.

Updates on Network and Service Status

5.6 During the recovery stage, the operator concerned should inform OFCA of the status of the affected network/service. Under critical circumstances, OFCA may specify the update frequency and the information to be provided by the operator concerned to facilitate the assessment on the impact of the incident/violation and the progress of recovery of the affected service.

Submission of Incident Report

5.7 Where requested by OFCA, ~~T~~the operator concerned should submit a preliminary report to OFCA within three working days after~~from the close of~~ the severe security incident/violation (or on such other date as specified by OFCA). The preliminary report should ~~give a detailed account of the security incident/violation in question, the impact caused by the incident/violation and the remedial action taken.~~ include the following information –

(a) description of the incident/violation;
(b) date and time of onset of the incident/violation;
(c) events which lead to the occurrence of the incident/violation;
(d) affected services;
(e) number of customers/end-users affected;
(f) affected area(s);
(g) remedial actions taken; and
(h) communications with OFCA, customers and the public.

5.8 Where requested by OFCA, a full report should be submitted to OFCA within 14 working days from the close of the incident/violation or on such other ~~deadline~~ date as specified by OFCA. In addition to item (a) to (h) of paragraph 5.7 above, ~~T~~the full report should give a detailed account of the measures which have been taken (or will be taken) in order to prevent recurrence of similar incidents/violations.

Contact Points

5.9 OFCA's contact points for reporting severe security incident/violation are as follows –~~-~~

	Tel. No.	**Email**
First Contact	✂	✂
Second Contact	✂	✂

Other general enquiries should be made to net_security@ofca.gov.hk.

5.10 Each operator is required to provide OFCA with the contact information of its focal point responsible for reporting severe security incident/violation, including the names, fixed and mobile Hong Kong telephone numbers and email addresses of the first and second contact persons. Whenever there is any update on the contact information, the operator should inform OFCA of the change at least five days before the effective date.

5.11 The main steps for reporting severe network security incident/violation are depicted in the flowchart at **Annex 4**.

~~Internet~~ Network/Service Outage and Wi-Fi Security Incident

5.12 OFCA has published guidelines for reporting network/service outages~~Internet outage/service degradation~~ and guidelines for public Wi-Fi security~~ in 2007~~[4]. Where incidents/violations fall within the pre-defined reporting criteria stipulated in those guidelines, relevant ~~Internet service providers and~~ operators should, in addition to alerting their customers, report the incidents/violations to OFCA within the specified timeframes. The said incident reporting mechanisms are applicable to any severe security incident/violation causing outage and/or service degradation in the NGN that provides telecommunications services.

Other Security Issues

5.13 If the security incident/violation is suspected to involve criminal

[4] "Guidelines for ~~Cable-based External Fixed~~ Telecommunications ~~Network Services~~ Operators ~~and Internet Service Providers~~ for Reporting Network/~~ and~~ Service Outage~~s~~ and Emergency Incident" can be downloaded at [To be updated]~~http://www.coms-auth.hk/filemanager/statement/en/upload/286/gn_201403e.pdf~~ and "Guidelines on the Security Aspects for the Design, Implementation, Management and Operation of Public Wi-Fi Service" can be downloaded at http://www.coms-auth.hk/filemanager/statement/en/upload/388/gn182016e.pdf.

offences, the operator concerned should report the case to the Hong Kong Police Force, the Customs and Excise Department or other relevant Government agencies, as appropriate, and provide necessary assistance for investigation.

SECTION 6: REPORTING OF NGN DEVELOPMENT STATUS AND SUBMISSION OF COMPLIANCE CHECKLIST

Reporting of NGN Development Status

6.1 From time to time, OFCA is requested by the International Telecommunication Union ("ITU") to submit regular returns on telecommunications development in Hong Kong including NGN development. To facilitate effective monitoring of operators' NGN development status by OFCA and also to ensure that the information provided to ITU would accurately reflect Hong Kong's position, operators should submit to OFCA their NGN development status on an annual basis within a specified timeframe. A template of the status report is at **Annex 5**.

Submission of Compliance Checklist

6.2 With a view to safeguarding telecommunications network security and enhancing protection of critical infrastructure, operators should conduct regular health check by completing, on an annual basis, a checklist at **Annex 6** about their compliance with the security and user protection measures set out in Sections 3 and 4 respectively. The completed checklist together with relevant supplementary information and supporting documents (if any) should be submitted to OFCA on an annual basis within a specified timeframe. Where requested by OFCA, operators should provide a more detailed account of their progress of compliance with specific measures.

6.3 OFCA will publish a summary highlighting those operators which have conducted the annual health check and confirmed the overall compliance with the associated security requirements in an appropriate format for information of the public.

SECTION ~~6~~7: REFERENCES

- ITU-T: Recommendation X.800: Security Architecture for Open Systems Interconnection CCITT Applications (03/1991)

- ITU-T: Recommendation X.805: Security Architecture for Systems Providing End-to-end Communications (10/2003)

- ITU-T: Recommendation Y.2701: Security Requirements for NGN (04/2007)

- ITU-T: Recommendation E.408: Telecommunication networks security requirements (05/2004)

- ITU-T: Security In Telecommunications and Information Technology (06/2006)

- ITU-T: Recommendation X.1038: Security requirements and reference architecture for software-defined networking (10/2016)

- ITU-T: Recommendation X.1601: Security framework for cloud computing (10/2015)

- OGCIO: Baseline IT Security Policy (S17), Version 3.1 (November 2008)

- OGCIO: IT Security Guidelines (G3), Version 5.1 (November 2008)

- CERT: Home Network Security (27 February 2006)

- 3GPP: Security Principles and Objectives, 3G TS 33.120 Version 3.0.0 (March 1999)

- 3GPP: Security Threats and Requirements, 3G TS 21.133 Version 3.1.0 (December 1999)

- 3GPP: A Guide to 3rd Generation Security, 3G TR 33.900 Version 1.2.0 (January 2000)

- 3GPP: Security Architecture, 3G TS 33.102 Version 3.7.0 (December 2000)

- NIST: Federal Information Technology Security Assessment Framework (28 November 2000)

- NIST: Telecommunications Security Guidelines for Telecommunications Management Network (Special Publication 800-13)

- NIST: Minimum Security Requirements for Federal Information and Information Systems (FIPS PUB 200, March 2006)

- NIST: Recommended Security Controls for Federal Information Systems (Special Publication 800-53 Rev 3, August 2009)

- NIST: Engineering Principles for Information Technology Security (A Baseline for Achieving Security) (Special Publication 800-27 Rev A, June 2004)

- NIST: Underlying Technical Models for Information Technology Security (Special Publication 800-33, December 2001)

- TISPAN: NGN Security (NGN_SEC) Requirements, Release 1

- TISPAN: NGN Security architecture, Version 0.015

- OECD: Guidelines for the Security of Information Systems and Networks (25 July 2002)

- ISO: 27001 Information technology – Security techniques – Information security management systems – Requirements

- NGMN: 5G security recommendations Package #2: Network Slicing (Version 1.0, 27 April 2016)

- NGMN: 5G security – Package 3: Mobile Edge Computing/Low Latency/Consistent User Experience (Version 2.0, 20 February 2018)

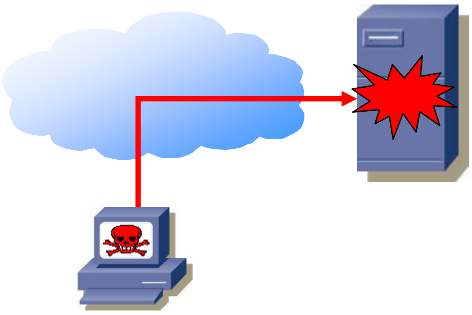
- ETSI: TS 103 487 v1.1.1: Baseline security requirements regarding sensitive functions for NFV and related platforms (2016-04)

Annex 1

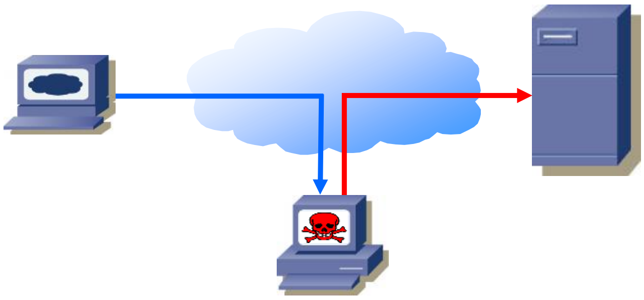
Security Threats against NGN

The architecture identifies security issues that need to be addressed in order to prevent both intentional and accidental threats.

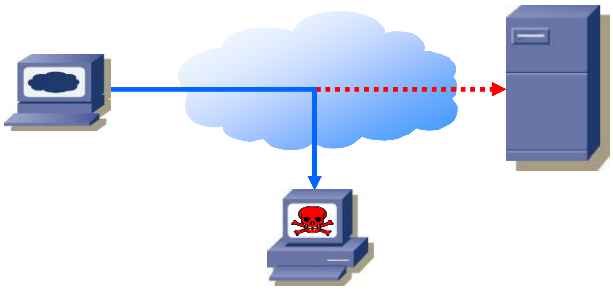
- Destruction – an attack on availability refers to the destruction of information and/or network resources



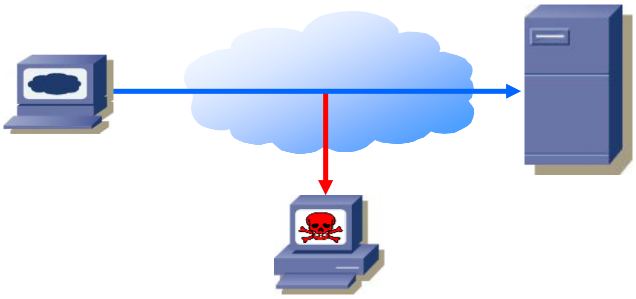
- Corruption – an attack on integrity refers to unauthorised tampering with an asset



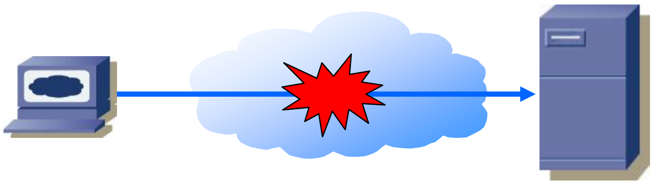
- Removal – an attack on availability refers to theft, removal or loss of information and/or other resources



- Disclosure – an attack on confidentiality refers to unauthorised access to an asset



- Interruption – an attack on availability refers to network becomes unavailable or unusable



Annex 2

Security Dimensions for Protection of NGN

The security dimensions shown below outline the security protections that can be deployed to counter security threats/attacks.

1. **Access Control** – It protects against unauthorised use of network resources. Access control ensures that only authorised personnel or devices are allowed access to network elements, stored information, information flows, services and applications. Examples of access control include the implementation of password, access control list ("ACL"), and firewall.

2. **Authentication** – It serves to confirm the identities of communicating entities. Authentication ensures the validity of the claimed identities of the entities participating in communication (e.g., person, device, service or application) and provides assurance that an entity is not attempting a masquerade or unauthorised replay of a previous communication. Examples of authentication are the use of shared secret, Public Key Infrastructure ("PKI"), Pre-shared Key ("PSK"), digital signature, and digital certificate.

3. **Non-repudiation** – It provides means for preventing an individual or entity from denying having performed a particular action related to data by making available proof of various network-related actions such as proof of obligation, intent, or commitment; proof of data origin, proof of ownership, proof of resource use. It ensures the availability of evidence that can be presented to a third party and used to prove that some kind of event or action has taken place. Examples of non-repudiation are the introduction of system logs and digital signatures.

4. **Data Confidentiality** – It protects data from unauthorised disclosure. Data confidentiality ensures that the data content cannot be understood by unauthorised entities. Encryption, access control lists, and file

permissions are methods often used to provide data confidentiality. Examples of cryptographic algorithms used for data encryption are Advanced Encryption Standard (“AES”), triple Data Encryption Algorithm (“3DES”) and Rivest-Shamir-Adleman (“RSA”).

5. **Communication Security** – It ensures that information flows only between the authorised end points. The information is not diverted or intercepted as it flows between these end points. Examples of communication security are the support of VPN, multiprotocol label switching (“MPLS”), Internet Protocol Security (“IPsec”), Transport Layer Security (“TLS”) / SSL and Hypertext Transfer Protocol Secure (“HTTPS”) and Layer 2 Tunnelling Protocol (“L2TP”).

6. **Data Integrity** – It ensures the correctness or accuracy of data. The data is protected against unauthorised modification, deletion, creation, and replication and provides an indication of these unauthorised activities. Examples of data integrity are the employment of Message-Digest algorithm 5 (“MD5”), Secure Hash Algorithms (“SHA”), message authentication code (“MAC”), keyed-Hash message Authentication Code (“HMAC”), digital signature, and anti-virus software.

7. **Availability** – It ensures that there is no denial of authorised access to network elements, stored information, information flows, services and applications due to events impacting the network. Examples of availability are the implementation of intrusion detection/protection system, network redundancy and business continuity/disaster recovery plan.

8. **Privacy** – It provides for the protection of information that might be derived from the observation of network activities. The information may include websites that a user has visited, a user’s geographic location, and the IP addresses and domain names of devices in a service provider network. Examples of privacy are the use of network address translation (“NAT”) and encryption.

Annex 3

User Best Practices for Accessing NGN

Users are encouraged to follow the best practices below when accessing the public telecommunications services –~~-~~

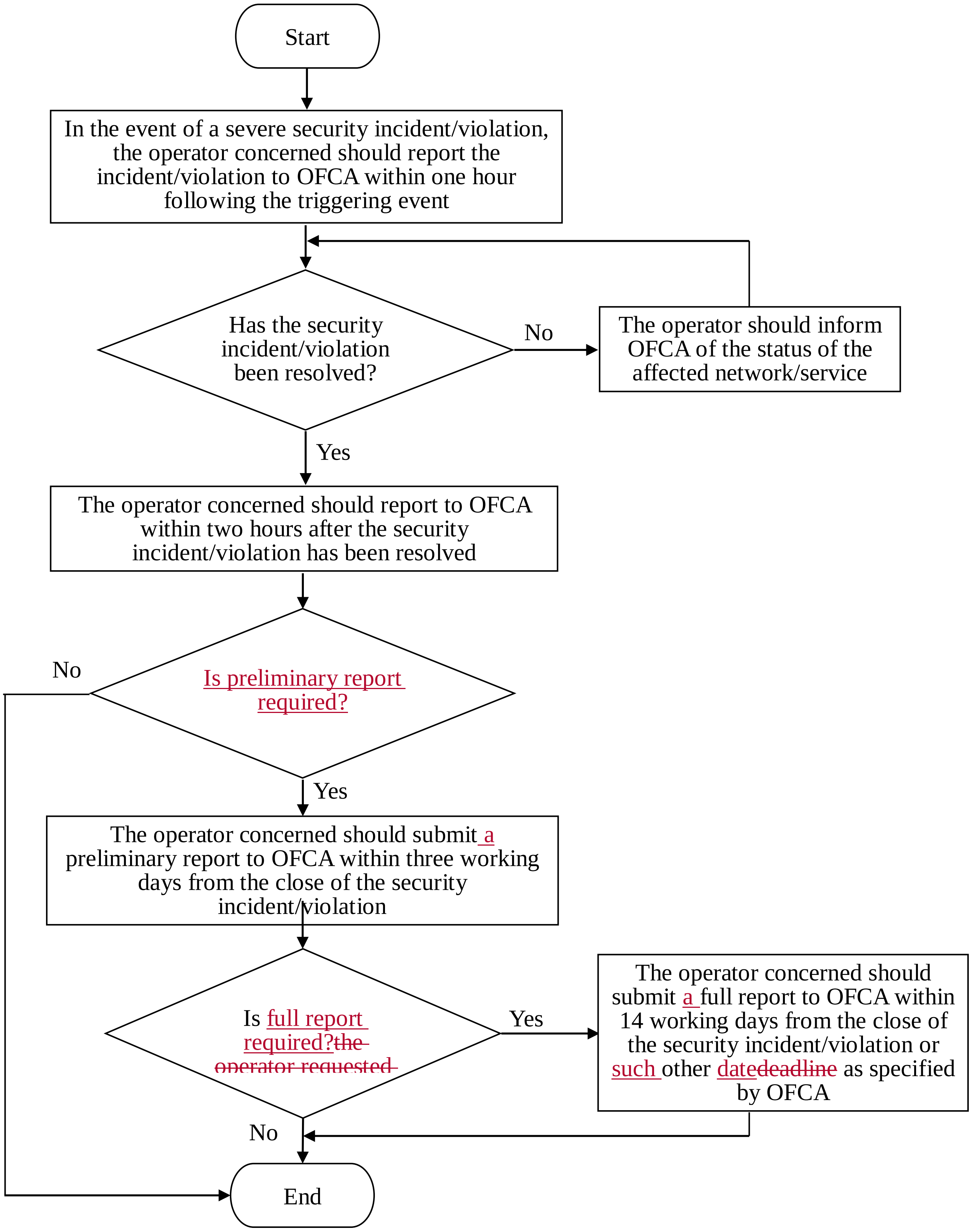
- keep security patches and network interface card drivers installed on the device up-to-date;
- backup all personal data on a regular basis;
- make a boot disk to aid in recovering from a security breach or hard disk failure;
- install and enable personal firewall, anti-virus and anti-spyware software and keep the associated definition files and security patches up-to-date;
- perform virus scan on removable disk and files downloaded from Internet before using them;
- encrypt sensitive data stored in the device accessing public telecommunications services;
- pack information or information backup in separate bag from the laptop in case of theft if travelling with confidential information;
- turn off the computer/notebook or disconnect from the network when not in use;
- set Internet connection default to ‘manual’ mode instead of ‘automatic’ mode;
- employ VPN technologies for enhanced end-to-end transmission protection;
- use a strong password that is difficult to guess but easy to remember. Change the password frequently;
- use different sets of login names and strong passwords for different services. Change the passwords on a regular basis;
- do not use hard-coded usernames and weak passwords;
- use multi-factor authentication, biometrics and identity management technology, etc. if provided by the service provider to strengthen

security for access to its network facilities/assets/systems/ equipment;

- report abnormal behaviour to your service provider or ISP immediately;
- disable Java, JavaScript, and ActiveX if possible;
- disable scripting features in email programs;
- disable hidden filename extensions;
- do not use any device which is infected by virus/malicious code;
- do not open any suspicious email and unknown email attachments;
- do not store any personal or sensitive information on a computer that is shared with others;
- do not cache the login name and password; and
- do not download or accept programs and contents from unknown or untrusted sources.

Annex 4

Incident Reporting Flowchart


Start
In the event of a severe security incident/violation, the operator concerned should report the incident/violation to OFCA within one hour following the triggering event
Has the security incident/violation been resolved?
No
The operator should inform OFCA of the status of the affected network/service
Yes
The operator concerned should report to OFCA within two hours after the security incident/violation has been resolved
Is preliminary report required?
No
Yes
The operator concerned should submit a preliminary report to OFCA within three working days from the close of the security incident/violation
Is full report required?~~the operator requested~~
Yes
The operator concerned should submit a full report to OFCA within 14 working days from the close of the security incident/violation or such other date~~deadline~~ as specified by OFCA
No
End

Annex 5

Template of Report on NGN Development Status

✂

✂

Annex 6

Checklist on Compliance with Measures set out in Security Guidelines for Next Generation Networks

✂

✂

✂

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 and other applications that are essential for the normal functioning of the society and economy. 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. If the continuous, reliable and secure operation of IoT devices deployed for Hong Kong's critical applications is adversely affected by malicious attacks or other disruptions, this may cause serious harm to economic activities, public services, people's livelihood, and even national 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. To safeguard IoT device security, IoT service providers should conduct regular health check by completing a checklist about their compliance with the relevant best practices and measures set out in this CoP, and report their status to the Office of the Communications Authority ("OFCA") on an annual basis. In recognition of operators for their commitment to compliance with the relevant security measures and best practices for reliable and secure operation of networks/services, OFCA will publish a summary highlighting those operators which have conducted the annual health check and confirmed the overall compliance with the associated security requirements on OFCA's thematic webpage for information of the public. 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, and 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

[1] For example, IoT devices ~~would~~ should 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.

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;

(e) sensitive data (e.g. personal data, device identifiers, usernames, and 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**.

Submission of Compliance Checklist and Publication of Status Report

7. With a view to safeguarding IoT device security and enhancing protection of critical applications, IoT service providers should conduct regular health check by completing, on an annual basis, a checklist at **Annex C** about their compliance with the best practices and

risk assessment measures set out in paragraph 5 and **Annex B** respectively. The completed checklist together with relevant supplementary information and supporting documents (if any) should be submitted to OFCA on an annual basis within a specified timeframe. Where requested by OFCA, IoT service providers should provide a more detailed account of their progress of compliance with specific best practice or risk assessment measure.

8. OFCA will publish a summary highlighting those operators which have conducted the annual health check and confirmed the overall compliance with the associated security requirements in an appropriate format for information of the public.

Application and Update of the CoP

9. 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.

10. 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~~MMMMM 2023

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.

Annex C

Checklist on Compliance with Best Practices and Measures set out in Code of Practice on the Operation and Management of Internet of Things 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 2.2~~1~~, GSM Association, 29 February 2020~~31 March 2019~~

"IoT Security Guidelines for IoT Service Ecosystem" Version 2.2~~1~~, GSM Association, 29 February 2020~~31 March 2019~~

"IoT Security Guidelines for IoT Endpoint Ecosystem" Version 2.2~~1~~, GSM Association, 29 February 2020~~31 March 2019~~

"IoT Security Guidelines for Network Operators" Version 2.2~~1~~, GSM Association, 29 February 2020~~31 March 2019~~

"IoT Security ~~Compliance~~ Assurance Framework" Release 3~~2~~, IoT Security Foundation, ~~December 2018~~November 2021

"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

*****