Tender Notice

T/2019/008: System Operation Contract S60: Operation of the Cyberport IT&T Infrastructure, Network Operation Centre (NOC) and Central Data Exchange (CDX)

Hong Kong Cyberport Management Company Limited ("HKCMCL") invites interested parties to submit tender for the Operation of the Cyberport IT&T Infrastructure, NOC and CDX **(**i.e. System Operation Contract S60). The contract for the existing System Operation Contract S60 will expire on 14 July 2020. The objective of this tender is to appoint an operator to manage, operate, maintain and support the Cyberport IT&T infrastructure, NOC and CDX for the provision of IT&T services upon expiry of the existing System Operation Contract S60. Refer to Annex A (enclosed) for the tender brief.

Interested parties with relevant experience shall fill-in the Reply to Tender Notice and sign the Confidentiality and Non-Disclosure Agreement (NDA) (both enclosed), then send them to the following on or before **4 October 2019:**

By Post:
Hong Kong Cyberport Management Company Limited
Units 1102-04, Level 11, Cyberport 2,
100 Cyberport Road,
Hong Kong

Attn: Manager – Compliance and Procurement
Or by email: procurement@cyberport.hk
Or by fax : (852) 3027 0385

Interested parties with relevant experience shall obtain the tender document on HKCMCL website in the "Tender Notice" Section. Upon receiving the signed NDA, we will contact you for providing a password to open the tender document. The tender closing date is **6 November 2019 at 3:00 p.m.** (Hong Kong Time).

If the company does not submit a tender or decline for submission after having replied to this notice, the company may be suspended from quotation for a period of time.

All costs and expenses incurred for or in connection with any response to this invitation, including the preparation of any submission, shall be borne entirely by the party concerned without recourse to HKCMCL.

Please note that submissions are being invited on a non-committal basis and this Invitation does not constitute any part of an offer by HKCMCL. HKCMCL is not bound to award any contract to any of those parties which have replied to this notice.

Date of Issue: [26 September 2019]

Reply to Tender Notice

T/2019/008: System Operation Contract S60: Operation of the Cyberport IT&T Infrastructure, Network Operation Centre (NOC) and Central Data Exchange (CDX)

Please complete and return this form to HKCMCL by email, by fax or by post ***no later than 4 October 2019****.*

By post	:	Units 1102-1104, Level 11, Cyberport 2, 100 Cyberport Road, Hong Kong
By fax	:	(852) 3027 0385
By email	:	procurement@cyberport.hk

We are interested to tender. Please see enclosed our 'Confidentiality and Non-Disclosure Undertaking' and provide us the password to open the tender document.

(If the tenderer does not submit a tender or decline for submission after have replied to HKCMCL with this form, the tenderer will be suspended from quotation for 3 months.)

Name in block letters: _____

Company name: _____

Company address: _____

_____

Tel. no.: _____

Fax. no.: _____

E-mail address: _____

Signature and company chop

_____ Date: _____

CONFIDENTIALITY AND NON-DISCLOSURE UNDERTAKING

This Undertaking is given by the undersigned in favour of Hong Kong Cyberport Management Company Limited (HKCMCL) in consideration of HKCMCL agreeing to supply to the undersigned copies of the Notes to Tenderer, Conditions of Tender, Articles of Agreement, General Conditions of Contract and Request for Proposal (collectively the "Tender Documents") for the tender of System Operation Contract S60: Operation of the Cyberport IT&T Infrastructure, Network Operation Centre (NOC) and Central Data Exchange (CDX) and to allow the undersigned to carry out a further study and prepare a proposal in response and pursuant to the Tender Documents (the Authorised Purpose).

NOW THEREFORE, the undersigned hereby agrees and undertakes as follows:-

1 In the course of carrying out the Authorised Purpose, the undersigned may have access to information or materials which is proprietary or confidential to HKCMCL or to third parties to whom HKCMCL owes a duty of confidentiality, including but not limited to materials describing or relating to the business affairs, policies or procedures of HKCMCL or such third parties, formulas, strategies, methods, processes, personal data, computer materials, including source or object codes, data files, computer listings, computer programs, and other computer materials (regardless of the medium in which they are stored), or other information.

2 All communications or data, in any form, which are disclosed by HKCMCL to the undersigned or obtained by the undersigned pursuant to or in connection with the Tender Documents or the Authorised Purpose and which are to be protected hereunder shall be considered as "Confidential Information".

3 For the purpose of this Undertaking, Confidential Information includes all information or data, whether written, oral or in any other tangible form, concerning HKCMCL which is furnished to the undersigned by or on behalf of HKCMCL, whether before or after the date of this Undertaking.

4 This Undertaking will terminate five (5) years from the date of signing.

5 The undersigned undertakes and agrees that any Confidential Information disclosed hereunder shall be used by the undersigned solely for the Authorised Purpose and except as may be required by applicable law or, by any supervisory or regulatory body in any jurisdiction, the undersigned will not disclose or disseminate such Confidential Information to anyone, except to those employees (including employees of its parent, subsidiaries and affiliates) and professional advisers who have a need to know such Confidential Information for the purpose for which it is disclosed

6. The undersigned shall use all reasonable safeguards against the unauthorized disclosure of Confidential Information and shall ensure that all of its employees and professional advisers having access to Confidential Information adhere to the terms of this undertaking as if they were a party hereto.

7 All material containing in the Confidential Information shall remain the property of HKCMCL. HKCMCL shall retain all right, title and interest in and to the Confidential Information. No licence under any trademark, patent, copyright, or any other intellectual property right, is granted or implied by the disclosure of any Confidential Information.

8 Notwithstanding anything in this Undertaking to the contrary, HKCMCL does not make any representations or warranties of any nature whatsoever with respect to any information disclosed, including, without limitation, any warranties of merchantability or fitness for a particular purpose or against infringement, the accuracy or completeness of the Confidential Information and shall incur no liability to the other or any other person resulting from the use of the Confidential Information.

9 The undersigned acknowledges that in the event of an unauthorized disclosure or any breach of this Undertaking by the undersigned could cause irreparable injury to HKCMCL, the damages incurred by HKCMCL may be difficult if not impossible to ascertain, and that HKCMCL may seek injunctive relief as well as monetary damages against the undersigned that breaches this Undertaking. The undersigned will pay all costs incurred in enforcing this Undertaking, including attorney fees, to HKCMCL.

10 Upon expiration of the period of confidentiality, or sooner upon written request of HKCMCL, all Confidential Information in the possession of the undersigned shall be returned to HKCMCL or destroyed, at the option and instruction of HKCMCL.

11 This Undertaking shall be governed by and construed in accordance with the laws of Hong Kong Special Administrative Region ("HKSAR") and the undersigned agree to submit to the non-exclusive jurisdiction of the courts of HKSAR.

Dated this ____day of _____ 2019

SIGNED)
By)
)
for and on behalf of)
[Company Name]) _____
)
)

)
_____)
in the presence of)
as Witness)

Annex A

Background & Tender Brief

1. Background

To fulfil Cyberport's public mission, a state-of-art IT&T infrastructure (including NOC and CDX, Appendix 1 refers) was built during the initial development stage of Cyberport for providing IT&T services (Appendix 2 refers) to Cyberport tenants and guests. Hong Kong Cyberport Management Company Limited (HKCMCL) has outsourced the operation, maintenance and support of the IT&T infrastructure to an operator via the S60 Contract since 2002.

2. Scope

The scope of the S60 Contract includes:

- Provision of manpower (please refer to Appendix 3 for the existing organisation chart), tools and required processes of IT&T services; and
- operation and maintenance of IT&T infrastructure (i.e. the basic equipment, structure and software incl. NOC and CDX to provide the IT&T services). There are over 3,000 equipment under the Contract.

The Operator is required to manage, operate, maintain and support the Cyberport IT&T Infrastructure as well as provide support to in-house IT operation of all HKCMCL's and/or its affiliated operations. For example, Smart-Space, HKCMCL's offices, Entrepreneurship Centre, Technology Centre, gym at IT Street, HKCMCL's corporate website, etc. The Operator is also required to provide IT supports for seasonal events and other special events as instructed by HKCMCL from time to time.

2.1. People

The NOC facilities shall be operational 24 hours a day, 7 days a week. It is assumed that some staffing will be provided by the Operator and/or third parties (for specific systems and levels of security) in addition to the 24/7 on-site staffing (Core Staff) provided by the Operator.

In addition to Core Staff for operating the NOC, the Operator shall reserve a pool of floating staff (Floating Staff) for periods when on-site staff are sick, on holiday or otherwise unavailable.

The minimum requirements in the new Contract of staff levels and the qualification and working experience of each rank of staff have been specified in Appendix 4. Please note that it is minimum requirements. After studying the current situation, the Operator shall propose a organization structure meeting Cyberport's business needs for next four years.

The Operator shall provide full support to the Core Staff on any technical issue and the Support Team will provide 2nd tier support for the Core Staff. If the Core Staff are unable to resolve any problem, the Support Team shall provide the necessary backup resources, technical advice and support to the Core Staff. The Support Team shall possess technical skills and expertise at least equivalent to that of the Core Staff in Cyberport. In addition to providing support to the Core Staff by the Support Team, the Operator shall also provide the Core Staff with all relevant and necessary backup resources including systems, tools, manuals and training.

2.2. Process

ITIL Processes The Operator shall bring under one roof the provision of IT&T systems management, NOC/IT services and support, NOC/network services and support and on-site services, project management, etc. The Operator shall provide IT services management solution to HKCMCL with full suite of Information Technology Infrastructure Library (ITIL) application. It shall cover, but not limited to, request fulfilment, change management, incident management and problem management processes.

ISO27001, CAS STAR and ISO9001 An Information Security Management System (ISMS) and a quality management system has been implemented and certified in compliance with ISO27001:2013 and ISO9001:2015 standards respectively. In addition to these two certificates, the Cyberport Community Cloud platform has been certified in compliance with Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR). The Operator shall continue to maintain and/or re-certify these three certificates. It includes, but not limited to, follow-up reviews or audits to confirm that the organization remains in compliance with the standard. Continuing maintenance requires periodic re-assessment and re-certification audits along with all other related activities to confirm that the ISMS and the quality management system continues to operate as specified and intended.

2.3. Tools

The NOC is functioning as a monitoring, service and control area for all IT&T services and transmit/receive paths to and from Cyberport. These include IPN (Internal Private Network) status

monitoring and control, Wi-Fi network status monitoring and control, cloud computing platforms monitoring and control, SMATV monitoring and control, IP Telephony monitoring and control, physical access system (i.e. iris recognition, fingerprint scanning and alphanumeric keyboard data entry monitoring) for NOC and CDX, network security control and CCTV (Closed Circuit TV) monitoring for NOC and CDX.

Ticketing System The NOC is using a ScienceLogic EM7 system for the incident/problem/change management and ticketing. Tickets are either created manually or generated by an event. Besides, the EM7 system is used for monitoring most of the network devices and servers in Cyberport while the Nagios is also used for monitoring of the network devices and servers. Please refer to Schedule 13 for the equipment being monitored by these two systems. The Operator shall propose a ticketing system/CRM replacing EM7 and Dynamics CRM to handle and record user request, and change/incident/problem management. The proposed system shall integrate with the Customer Data Management and other existing monitoring systems (i.e. Nagios, AirMagnet and NetFlow).

Customer Data Management The operation of the Help Desk shall be in the NOC. The Customer Data Management and associated systems shall allow users to access support. The support systems for the help center, such as the call centre, ticketing system, monitoring tools, asset management system and Customer Data Management system, are described in further detail below and in the appendices. The NOC is currently using a Microsoft Dynamics CRM 2016 On-Premises system for managing the customer data.

Assets Management Microsoft Excel is being used by the existing Operator to manage the equipment and spare parts inventory. To enhance services to meet the growth demand, the new Operator shall provide an asset management system to assist NOC staff to manage the equipment and spare parts inventory. It can be an addon module of the CRM or Ticketing system or a separate system integrated with the CRM/Ticketing system.

All these monitoring tools, except EM7 and Dynamics CRM, are owned by HKCMCL. EM7 and Dynamics CRM are provided by the existing Operator as a service. The new Operator should provide a replacement for these tools.

Password Management System The existing Operator is currently using a Pleasant password server for the management of the password of privileged accounts for the device, system and servers. It is considered to replace it with a more powerful Password Management System to meet the operational needs. The new system can auto check passwords, change passwords every set period and allow NOC staff logging into a system without ever showing the password.

Monitoring Tools In additional to EM7 and Nagios, the following monitoring tools are being used to monitor the various aspects as stated below:

- NetFlow Tracker for network traffic monitoring
- AirMagnet for Wi-Fi network monitoring
- A dashboard is developed by Cacti and RRDtool for network traffic monitoring

2.4. Equipment Maintenance

The Operator shall purchase maintenance and support service from the original equipment manufacturer for the Equipment or the New System whenever the service is available, e.g. Cisco's SMARTnet Services for Cisco's equipment and Juniper's Juniper Care for Juniper's equipment. The service level should be 24 x 7 x 4 (24 hours per day, 7 days per week and 4 hours response time). HKCMCL can directly contact the original equipment manufacturer for the Equipment or the New System for any support or project matters with no cost to HKCMCL.

3. Service Level Agreements and KPIs

The Operator shall carry out preventive and corrective maintenance on the System so as to ensure that at all times the System will enable the Operator to meet the Service Level Agreements and Key Performance Indicators (KPI).

3.1. SLA

The Services shall be performed by the Operator in a manner and to a standard that will comply fully with the Service Levels in Appendix 5.

3.2. KPI

The Operator should take particular note of the details of the KPI and their associated performance measures to be met. This will also form a fundamental control and accountability mechanism for the Operator.

The table in Appendix 6 shows the high-level KPIs for Fiscal Year (FY) 2017/18. HKCMCL will review those KPIs every FY.

The Operator is encouraged to propose additional KPIs in operational level. The results implied by these operational KPIs are monitored by operational performance measures. They are the drivers of whole-process results and are where resources are allocated to improve process performance and ultimately improve organisational success and sustainability to achieve the high-level KPIs.

4. Handover/Transition Services

There is a Handover Period for the existing Operator to handover to the new Operator. During the Handover Period, the existing Operator will be responsible for continuing the service to the service standard and effecting the smooth handover.

The new Operator shall develop the Handover Plan in ensuring smooth Handover. As such, the new Operator shall obtain from time to time according to the Handover Plan from the Existing Operator all relevant information regarding management, operation and maintenance of the System. The Operator shall be fully conversant with and thoroughly understand how to manage, operate, maintain and support the System. The Operator shall also obtain from the Existing Operator all necessary information to be fully aware of all the details of the Services.

The previous 6-year S60 Contract with existing operator ended. Comparing to the previous S60 Contract, the new S60 Contract has additional requirements to cope with the growth of Cyberport and the increasing

demand from tenants (Appendix 7 refers). For meeting these additional requirements, the new Operator was required to complete all the transition services during the handover period.

The Handover exercise has the following additional goals:

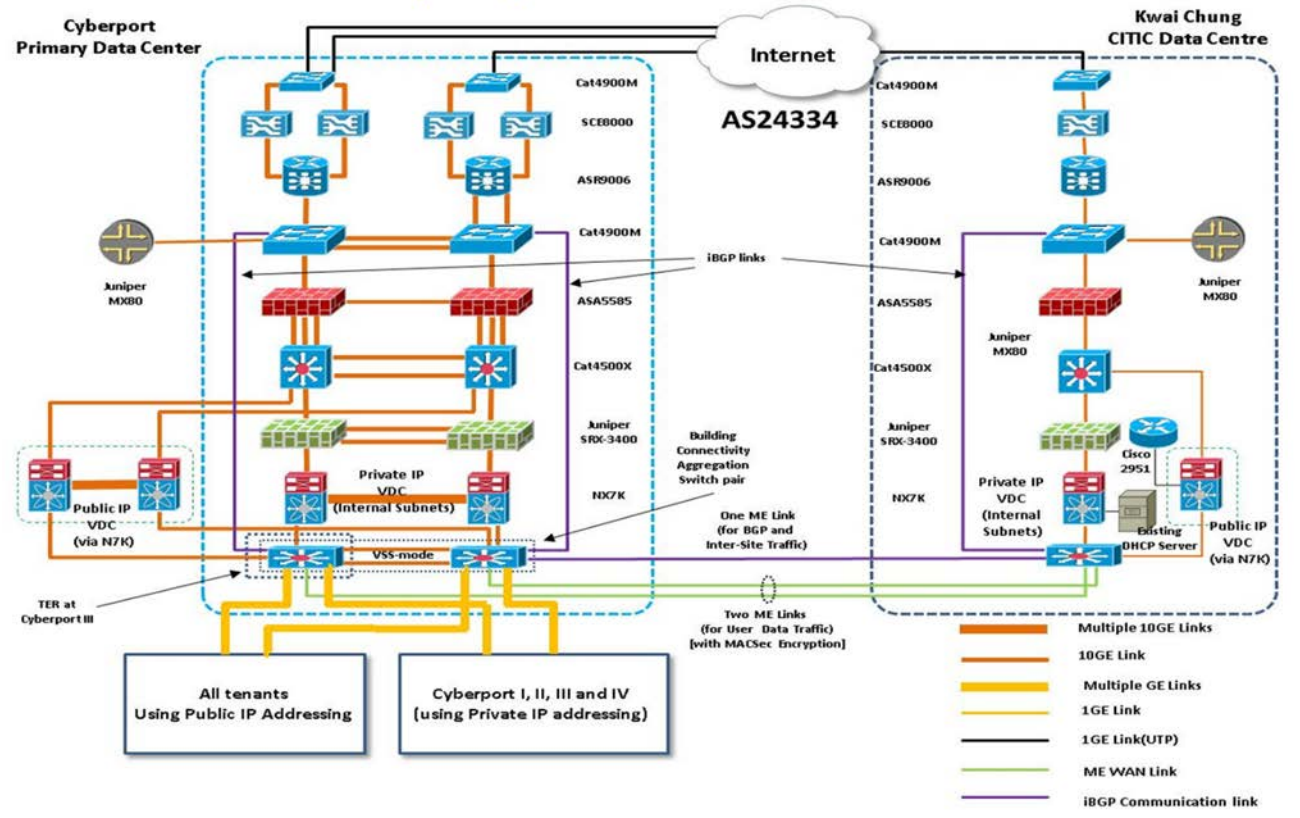
- To evolve the NOC and Service team capability through a resource realignment exercise;
- To review and revise current service operation process to better align with ITIL best practice and, no less importantly, align with Cyberport's business model and process flows; and
- To implement a customer record management system and a ticketing system. The CRM system should be integrated with the ticketing system. The existing ticking system (EM7) and CRM system were provided by the existing Operator.

5. Tentative Schedule

September – December 2019	Tender Exercise
December 2019	Contract Award
December 2019 to June 2020 (latest)	Handover Period
1 July 2020 (latest)	Cut-off Date

Cyberport IT&T Infrastructure

Cyberport Core Network



Appendix 2

Cyberport IT&T Services

Internal Private Network

- The Internal Private Network (IPN) is Cyberport's backbone for Internet access. IPN is a unique IT&T facility provided by HKCMCL to community members at Cyberport. Though it is an Internet product, it is different from those broadband products available in the market. Cyberport has all its areas covered by Cyberport Optical Network (CON), through which tenants can subscribe for a guarantee international/local Internet bandwidth per Mbps (up to 1Gbps) on a monthly basis.
- **Two** IPN ports currently at **100** Mbps local shared bandwidth, free of monthly charge, can be provided to our community members (**dedicated international bandwidth** can be allocated at extra cost).

Cyberport Community Cloud

- Cyberport Community Cloud is the first-ever Community Cloud in Hong Kong. It offers easy-to-use and self-provisioning Infrastructure-as-a-Service (IaaS) to our community members. The platform is certified with CSA STAR certification.

Cyberport OpenWi-Fi

- Users enjoy FREE Wi-Fi connection for public areas (all major public areas in Cyberport are covered by WLAN).

Satellite Signal Downlink Services

- Cyberport is partnering with one of the Satellite-based Fixed Carrier Licensees to provide downlink services of encrypted video signal from satellite for Cyberport community members. Cyberport is receiving signal for eight satellites.

IP Telephony and Unified Messaging Service

- Cyberport is partnering with Hong Kong Broadband Network Ltd. (HKBN) to offer an IP based telephony and unified messaging service which integrates telephone, email and fax into one single interface.

Blockwiring Services

- Fixed Telecommunications Network Services (FTNS) providers or other Internet Services Providers (ISPs) are providing their Internet access services and fixed line telephone services to our tenants via the Blockwiring cabling infrastructure.

Satellite Master Antenna Television System (SMATV)

- 124 satellite TV channels are downlinked and delivered to tenants over the IPN via multicasting at 5Mbps to 20Mbps per channel.
- It is accessible from desktop, laptops or via television.

Network Operation Centre (NOC) and Central Data Exchange (CDX)

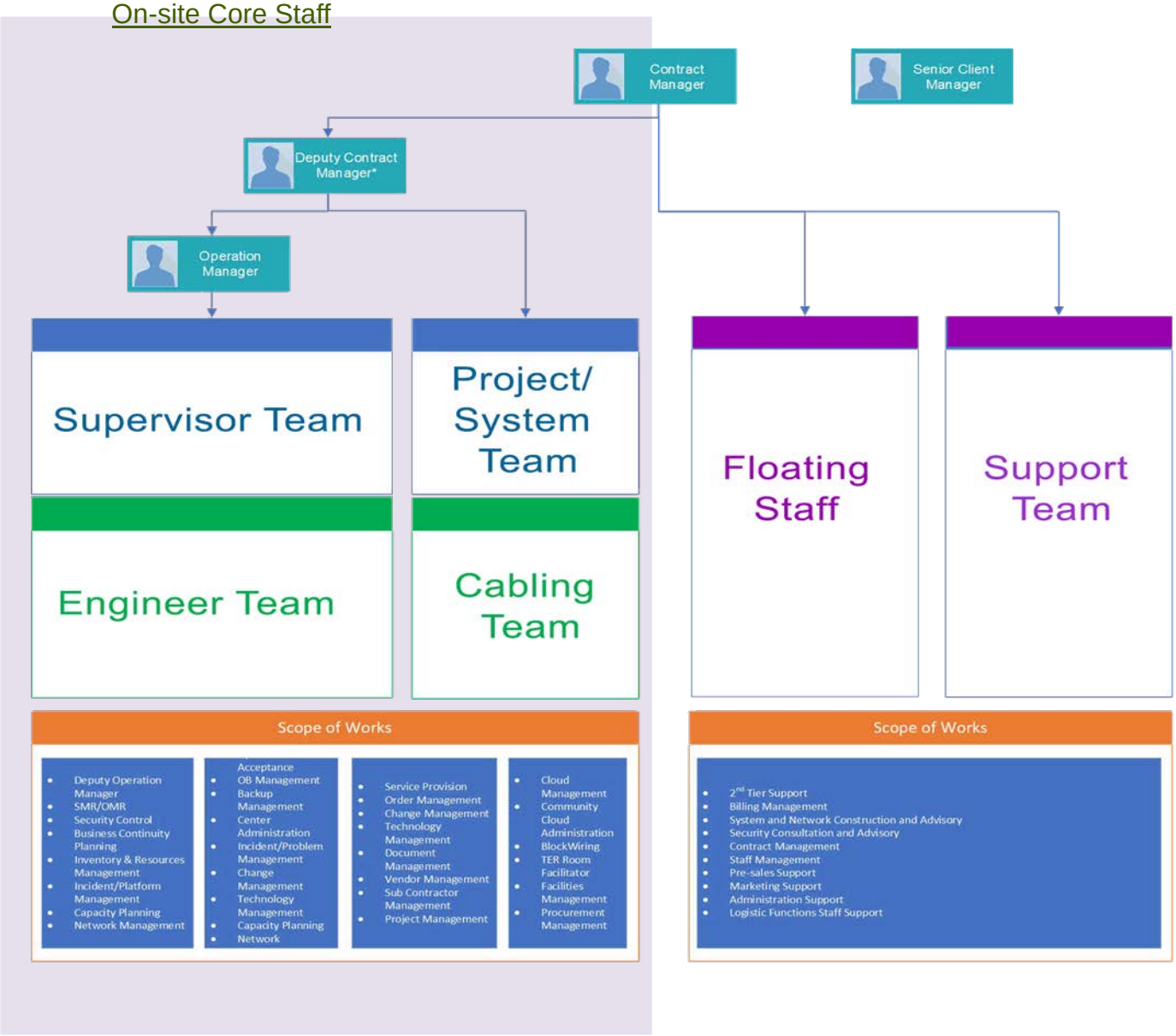
- NOC is the central monitoring and management centre for Cyberport's IT&T infrastructure. It consists of a Tier 3+ Data Centre with a fully redundant technical architecture and network design, which is certified with ISO 9001 and ISO 27001.
- In order to provide the best Information Security to our clients, our operation follows the requirements of the Information Security Best Practice under ISO27001.
- With a remote DR site provisioned in one of the major carrier grade data centres outside Cyberport, NOC can execute its business continuity plan in case local Cyberport NOC/CDX cannot operate.

Appendix 3

Cyberport IT&T Services

NOC and CDX's Existing Organisational Structure

On-site Core Staff



Minimum Qualification and Headcount Requirement for the Core Staff Specified in New S60 Contract

Section Content:	Minimum Qualification Requirement for the Core Staff

Core Staff (On-site)

Rank	Minimum Qualification Requirement	Minimum Years of Experience
Contract Manager (or equivalent)	• U Grad in Computer Science / Engineering, Information Systems or related disciplines; • Have at least one (1) professional IT certificate [(a)] ; and • Good command of both written and spoken Chinese (Cantonese/Mandarin) and English	• Have at least 15 years working experience; and • Have at least six (8) years working experience in team leading, including four (5) years of team leading experience in operation management of support team
Deputy Contract Manager (or equivalent)	• U Grad in Computer Science / Engineering, Information Systems or related disciplines; • Have at least one (1) professional IT certificate [(a)] ; and • Good command of both written and spoken Chinese	• Have at least 12 years working experience; and • Have at least six (6) years working experience in team leading, including four (4) years of team leading experience in operation management of support team
Operation Manager (or equivalent)	• U Grad in Computer Science / Engineering, Information Systems or related disciplines; • Have at least one (1) professional IT certificate [(a)] ; and • Good command of both written and spoken Chinese	• Have at least 10 years IT&T working experience [(b)]; and • Have at least six (6) years working experience in team leading, including four (4) years of team leading experience in operation management of support team
NOC Supervisor (or equivalent)	• U Grad in Computer Science / Engineering, Information Systems or related disciplines; • Have at least one (1) professional IT certificate (a) ; • Good command of both written and spoken Chinese; and • As a whole, the team of NOC Supervisor should have at least: o one (1) CCIE Routing and Switching certificate; and o one (1) JNCIE-SP certificate.	• Have at least five (5) years IT&T working experience [(b)] and • As a whole, at least one (1) NOC Supervisor with three (3) years OpenStack working experience; and • As a whole, at least one (1) NOC Supervisor should have at least four (4) years Ruckus Wireless System working experience.
NOC Engineer (or equivalent)	• U Grad in Computer Science / Engineering, Information Systems or related disciplines; • Have at least one professional IT certificate [(a)] • ; and • Good command of both written and spoken Chinese • As a whole, the team of NOC Engineer should have at least a total of: o one (1) CCNP Security certificate; and o three (3) CCNA certificates; and o one (1) JNCIP-SEC certificate; and o one (1) MCSE certificate	• Have at least two (2) years IT&T working experience. At least one of NOC Engineers with two (2) years OpenStack working experience
NOC Assistant Engineer (or equivalent)	• Diploma or Higher Diploma in Computer Science / Engineering, Information Systems or related disciplines; • Have at least one (1) professional IT certificate [(a)] ; and • Good command of both written and spoken Chinese OR	• Have at least one (1) year IT&T working experience [(b)] ; and • On average, the team of Engineers should have at least one (1) year IT&T working experience
	• U Grad in Computer Science / Engineering, Information Systems or related disciplines; and • Good command of both written and spoken Chinese	• On average, the team of Engineers should have at least one (1) year working experience
Cabling Engineer (or equivalent)	• Diploma or Higher Diploma in Engineering, Information Systems or related disciplines; ; and • Good command of both written and spoken Chinese	• Have at least 10 years structured cabling, IT networking working experience; and • Have at least 6 years working experience in team leading
Cabling Assistant Engineer (or equivalent)	• Level 2 or above in 5 subjects in the HKDSEE; or • Level 2 / Grade E or above in the HKCEE; and • Good command of both written and spoken Chinese	• Have at least 5 years structured cabling, IT networking working experience

Minimum Qualification and Headcount Requirement for the Floating Staff Specified in New S60 Contract

Floating Staff		
Rank	**Minimum Qualification Requirement (M)**	**Minimum Years of Experience (M)**
NOC Supervisor (or equivalent)	• U Grad in Computer Science / Engineering, Information Systems or related disciplines; • Have at least one professional IT certificate [(a)] ; and • Good command of both written and spoken Chinese	• Have at least five (5) years IT&T working experience [(b)]
NOC Engineer (or equivalent)	• U Grad in Computer Science / Engineering, Information Systems or related disciplines; • Have at least one (1) professional IT certificate [(a)] ; and • Good command of both written and spoken Chinese	• Have at least two (2) years IT&T working experience [(b)]
NOC Assistant Engineer (or equivalent)	• Diploma or Higher Diploma in Computer Science / Engineering, Information Systems or related disciplines; • Have at least one professional IT certificate [(a)] ; and • Good command of both written and spoken Chinese OR	• Have at least one (1) year IT&T working experience [(b)]; and • On average, the team of Engineers should have at least one (1) year working experience
	• U Grad in Computer Science / Engineering, Information Systems or related disciplines; and • Good command of both written and spoken Chinese	• On average, the team of Engineers should have at least one (1) year working experience

Note

(a) Certificates in IP networking, administration of Unix, Linux or Windows Server, IT security, IT service management or IT/Telecom related certificates.

(b) Working experience in IP networking, database administration, IT security or server management of Unix, Linux or Windows Server, Network/Data Security or related area.

Appendix 5

Service Level Agreements

Table 1 Service Levels for Overall Service Availability

No.	Service measures	Minimum Service Levels
1.	Overall Service Availability	>= 99.95% per month
2.	Number of Unscheduled Service Interruptions	<= 1 incident per month

Table 2 Service Availability for Individual Systems

No.	System	Minimum Service Levels
1.	Internal Private Network (IPN)	>= 99.95% per month
2.	Bandwidth on Demand (BoD)	>= 99.95% per month
3	Wireless Local Area Network (WLAN)	>= 99.95% per month
4	Cloud Computing Platform	>= 99.95% per month
5	Satellite Master Antenna Television System (SMATV)	>= 99.95% per month
6	Blockwiring (BW)	>= 99.95% per month
7	Network and Data Security and Firewall	
7.1	Virus Protection Service	>= 99.95% per month
7.2	Firewall	>= 99.95% per month
7.3	Intrusion Detection System / Intrusion Prevention System	>= 99.95% per month
7.4	Virtual Private Network (VPN)	>= 99.95% per month
8	Satellite Signal Downlink	>= 99.95% per month

Table 3 Service Levels for Response Time

No.	Service measures	Minimum Service Levels
1.	Call answer rate for voice	80% in 30 seconds
2.	Call abandon rate	5% of all incoming calls
3	Fax and e-mail inquiries	80% respond within 24 hours 100% respond within 48 hours

Table 4 Service Levels for Service Provision Lead-time

No.	System	Minimum Service Levels
1.	Internal Private Network (IPN)	<= 7 calendar days
2.	Bandwidth on Demand (BoD)	<= 4 hours
3	Cloud Computing Platform (Cloud)	<= 1 calendar days
4	Satellite Master Antenna Television System (SMATV) – add / remove / change channel	<= 3 calendar days
5	Blockwiring (BW)	<= 7 calendar days
6	Network and Data Security and Firewall	
6.1	Virus Protection Service - Provide solution to known virus	<= 2 hours
6.2	Firewall - Response time to critical security event - Update firewall rules	<= 2 hours <= 1 calendar days
6.3	Intrusion Detection System / Intrusion Prevention System - Response time to critical security event	<= 2 hours
6.4	Virtual Private Network (VPN)	<= 1 calendar days
7	Satellite Signal Downlink	<= 7 calendar days

Table 5 Service Levels for Time To Repair

No.	System	Severity Level	Minimum Service Levels (per month)
1.	Internal Private Network (IPN)	1	within 2 hours
		2	90% within 5 hours
		3 & 4	3 hours provide advice
2.	Bandwidth on Demand (BoD)	1	within 2 hours
		2	90% within 5 hours
		3 & 4	3 hours provide advice
3	Wireless Local Area Network (WLAN)	1	within 2 hours
		2	90% within 5 hours
		3 & 4	3 hours provide advice
4	Cloud Computing Platform (Cloud)	1	within 2 hours
		2	90% within 5 hours
		3 & 4	3 hours provide advice
5	Satellite Master Antenna Television System (SMATV)	1	within 2 hours
		2	90% within 5 hours
		3 & 4	3 hours provide advice
6	Blockwiring (BW)	1	within 2 hours
		2	90% within 5 hours
		3 & 4	3 hours provide advice
7	Network and Data Security and Firewall		
7.1	Virus Protection Service	1	Known Virus - 2 hours New Virus (simple case) - 4 hours New Virus (complex case) - 24 hours
		2	N/A
		3 & 4	N/A
7.2	Firewall	1	within 2 hours
		2	90% within 5 hours

No.	System	Severity Level	Minimum Service Levels (per month)
		3 & 4	3 hours provide advice
7.3	Intrusion Detection System / Intrusion Prevention System	1	within 2 hours
		2	90% within 5 hours
		3 & 4	3 hours provide advice
7.4	Virtual Private Network (VPN)	1	within 2 hours
		2	90% within 5 hours
		3 & 4	3 hours provide advice
8	Satellite Signal Downlink	1	within 2 hours
		2	90% within 5 hours
		3 & 4	3 hours provide advice

Table 6 Service Levels for Change Management Service

No.	Service measures	Minimum Service Levels
1.	Lead-time for prepare the change	<= 7 calendar days
2.	Change implementations per change schedule	98%
3	Successful implementation	>=99%

Appendix 6

KPIs for S60 Operation in FY2019/20

KPIs	FY2019/20 TARGET METRICS
Internet bandwidth: yearly average (year-over-year (YoY) growth rate)	>= 15%
IT&T Services Availability	>=99.95%
Meet Revenue Target of IT&T Services (YoY growth rate)	>=2%
Drive the Cloud Computing technology (New application on cloud platform by Cyberport tenants and current incubates)	>= 200
ISO 27001 External Audit (number of nonconformity)	0
ISO 9001 External Audit (number of nonconformity)	0
STAR External Audit (number of nonconformity)	0
Customer Satisfaction Rating	>= 80 and Maintain YoY
Core Staff (On-Site) Retention Rate: Monthly	>= 80%

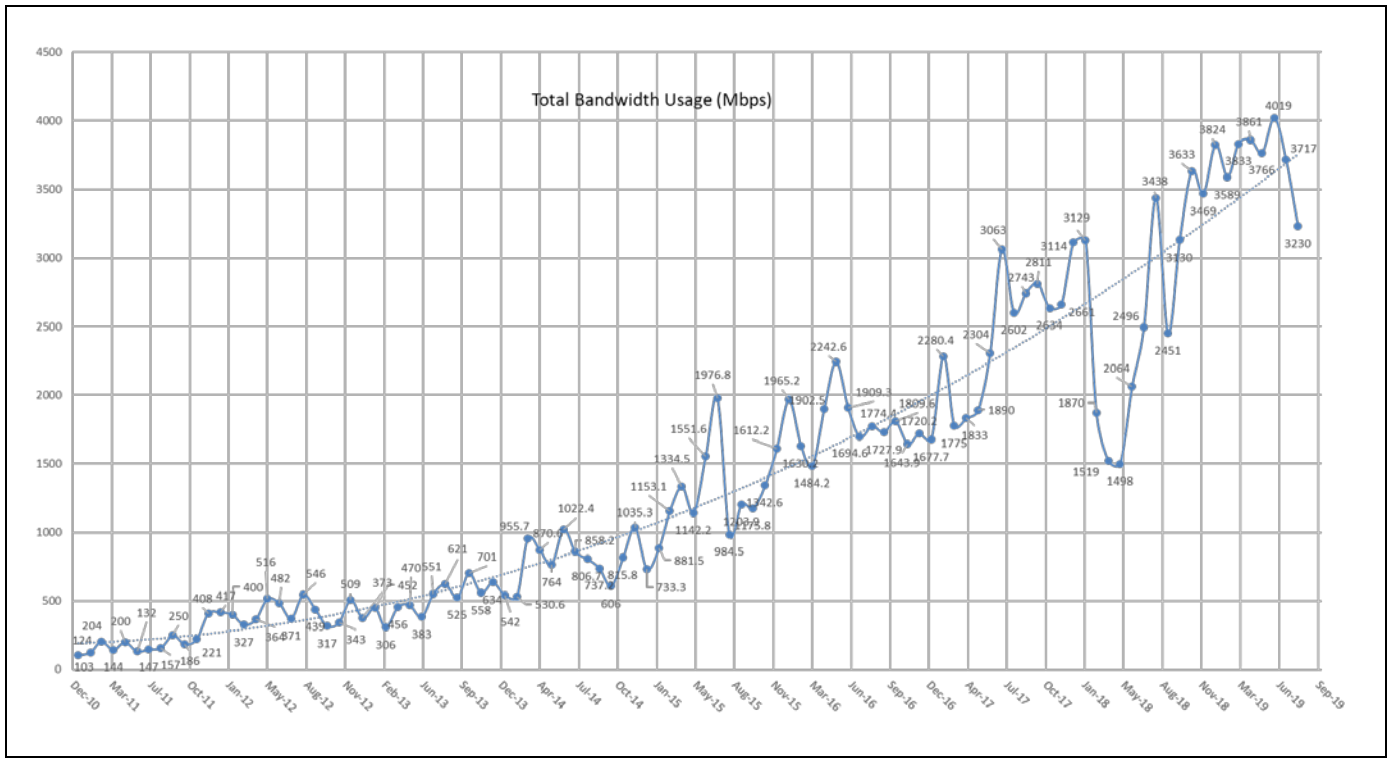
Appendix 7

Demand on IT&T Services

(i) The numbers of tickets issued and the number of changes handled increased drastically:

Year	Number of Tickets Issued [1]	Number of Changes Handled [2]
FY2012/13	132	530
FY2013/14	90	575
FY2014/15	268	546
FY2015/16	221	1091
FY2016/17	311	907
FY2017/18	718	627
FY2018/19	617	885

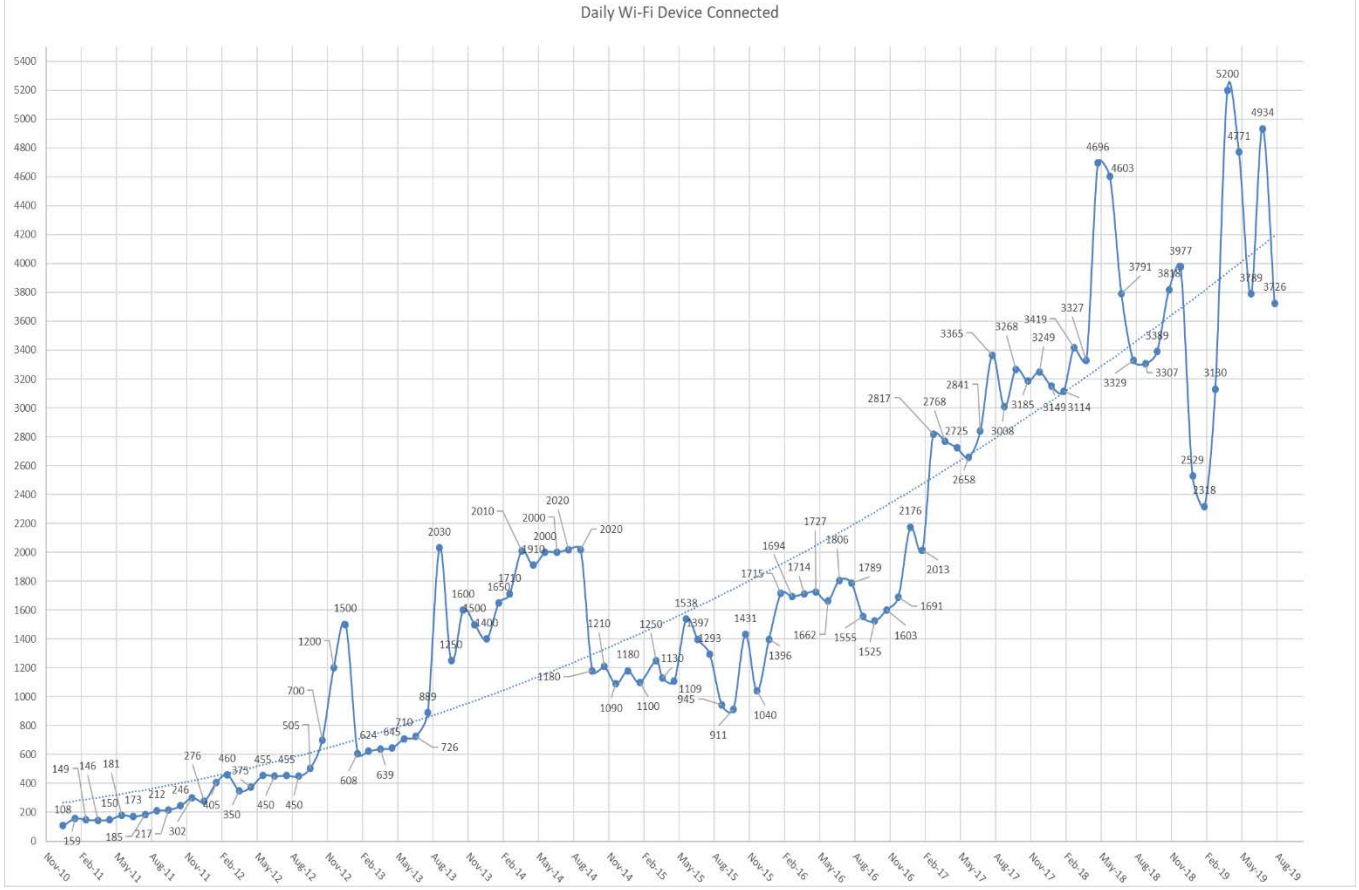
(ii) The total bandwidth usage increased from 124 Mbps in Jan 2011 to 3,230 Mbps in Aug 2019 (2,605%)

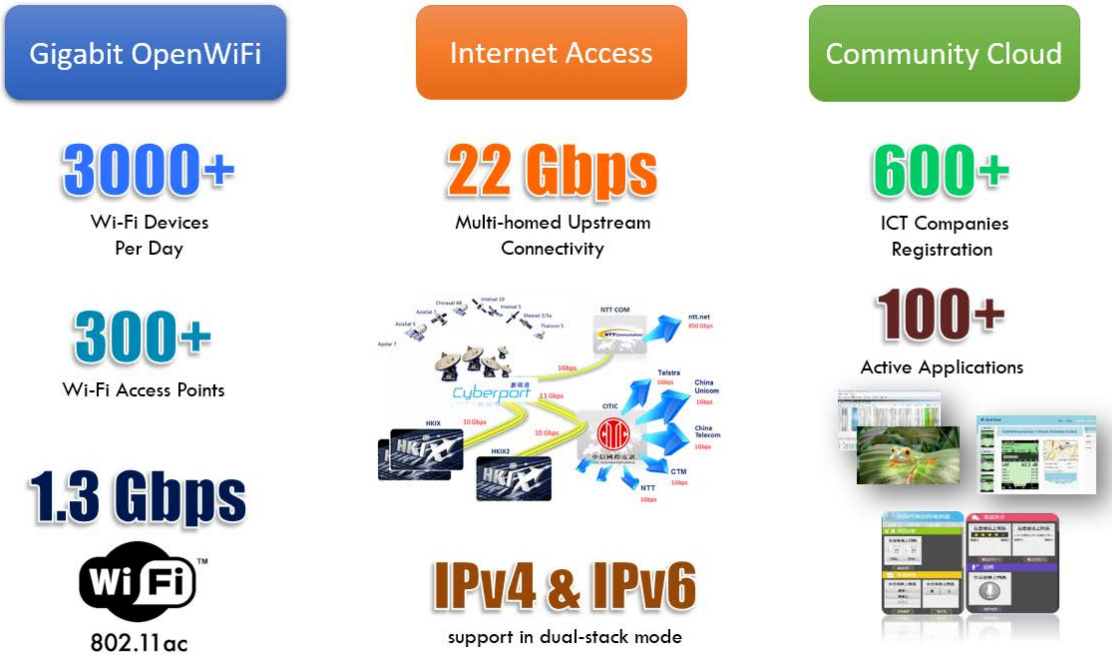


[1] Tickets refer to those incident tickets created in respect of incidents identified by monitoring tools or reported by end-users/customers. NOC should take follow up actions to ensure that the incidents are properly handled.

[2] Changes refer to all systems changes performed by NOC, either as standard system changes, or in response to incidents or IT service provision requests, or to align with other IT projects. NOC should ensure that all changes are recorded, evaluated, implemented, documented and reviewed in a controlled manner.

(iii) The number of daily wi-fi device connected increased from 159 in Jan 2011 to 3,726 in Aug 2019 (2,343%).





20