

LCQ2: Information technology support for government personnel working from home

Following is a question by the Hon Charles Mok and a written reply by the Secretary for Innovation and Technology, Mr Alfred Sit, in the Legislative Council today (May 13):

Question:

From January 29 to the end of April this year, the Government made arrangements for government personnel not providing emergency and essential public services to work from home. Regarding the details of the information technology support, such as newly installed or procured computers and other mobile devices/equipment and computer software as well as enhanced capacities of communications/networks/databases, provided by the various government departments to support their staff to work efficiently from home, will the Government inform this Council:

(1) of the details of the (i) computers and other mobile devices/equipment as well as (ii) computer software which were newly installed or procured by the various government departments (set out respectively in Tables 1 and 2);

Table 1

Name of department	Type of computers/devices/equipment	Brand and model number	General retail price	Supplier and unit purchase price	Purpose	Quantity	Expenditure account

Table 2

Name of department	Type of software	Brand, software name and version	General retail price	Supplier and unit purchase price	Purpose	Quantity	Expenditure account

(2) of the details of the enhancement made by the various government departments to the capacities of their communications/networks/databases (set out in Table 3);

Table 3

Name of department	Type	Enhancement percentage	Supplier/contractor	Purpose	Expenditure	Expenditure account

(3) of (i) the number of staff members who were newly authorised by the various government departments to access government intranets and servers through virtual private networks (VPNs) to facilitate their receipt and delivery of emails as well as their storage and retrieval of information (how such number compares with the relevant figure before implementation of the work-from-home arrangements), as well as (ii) the details of the enhancement made by the various government departments to the capacities of their VPN facilities (including the increase in the number of real time concurrent users allowed);

(4) of the respective numbers of staff members in the various government departments to whom notebook computers that can be connected to government intranets and servers were distributed (with a breakdown by rank);

(5) of the number of staff members who were newly authorised by the various government departments to access government intranets and servers for storing and retrieving government confidential information outside office, and how such number compares with the relevant figure before implementation of the work-from-home arrangements; and

(6) of the additional measures adopted to mitigate the information security risks arising from the implementation of the work-from-home arrangements for government personnel?

Reply:

President,

In consultation with policy bureaux and departments, our reply to the six-part question is set out below:

(1) and (2) To implement the work from home arrangement for government staff, government departments have procured additional computers and other mobile devices/equipment, computer software, and enhanced the capacities of their communications/networks/databases according to their operational and staffing demands. The relevant information is at Tables 1 to 3.

(3) Government departments have all along been arranging authorised staff to access their departmental intranets and servers by Virtual Private Network (VPN) for working remotely. Under the work from home arrangement due to the COVID-19 epidemic, between January 29 and end-April 2020, the number of staff authorised for using VPN increased by about 5 150. The number of real-time concurrent users has also increased by about 2 050.

(4) Between January 29 and end-April 2020, about 4 600 additional government staff were provided with notebook computers for accessing departmental

intranets and servers. We do not have the breakdown by rank.

(5) Between January 29 and end-April 2020, the number of staff authorised for accessing classified information outside their offices through equipment provided by the government and secure communications channels has increased by about 2 600.

(6) According to the Government IT Security Policy and Guidelines, while ensuring information security, departments can provide individual government staff with equipment such as notebook computers and mobile devices so that they can work from home by remotely accessing government systems and networks through secure communications channels (including encrypted VPN connections with two-factor authentication). Such equipment have installed security patches and anti-malware software which are regularly updated so as to guard against hacking or leakage of information. Relevant staff cannot store government classified data on their own computers and mobile devices.

In addition, all departments must arrange regular training like seminars and workshops to promote staff awareness of cyber security, covering information related to remote access to government systems and networks. The Office of the Government Chief Information Officer also reminds departments and their staff from time to time of cyber security information including awareness of phishing attacks and security precautions to take in using video conferencing, etc.