DPO’s response to media enquiries on government staff’s use of personal webmail, public cloud storage and web-version of instant messaging services

In response to media enquiries on government staff's use of personal webmail, public cloud storage and web-version of instant messaging services, a spokesman for the Digital Policy Office (DPO) said today (October 23):

In face of increasingly severe cyber threats, the DPO reminded all bureaux and departments (B/Ds) through the Government's IT Security Guidelines (the Guidelines) updated in April this year that their staff's use of personal webmail, public cloud storage and instant messaging services on desktop computers connected to the government internal network will bring potential information security risks, hence the risks must be well managed. In this regard, the DPO has formulated the following security guidelines for the use of desktop computers connected to the government internal network systems:

(1) Government staff have to obtain approval from department management before using personal webmail, public cloud storage and instant messaging services on desktop computers connected to the government internal network; and

(2) Based on operational needs, B/Ds can implement different alternatives during the six-month adaptation period after the promulgation of the Guidelines, including providing staff with mobile devices or designated computers that are isolated from the B/Ds' internal network system, so that they could continue using relevant personal webmail, public cloud storage and instant messaging services, or dedicated application systems developed by the B/Ds.

The above-mentioned Guidelines aim to strengthen the security barrier of the government internal information network system, and do not restrict or affect the use of relevant services (including WhatsApp, WeChat and other commonly used instant messaging softwares) by staff through mobile phones, mobile devices or other desktop computers that are independent of the government internal network system. There is no "blanket ban" on the use of relevant communication tools. The requirements of the Guidelines also do not apply to computer systems or communication devices that are not connected to the government internal network, such as on-campus systems in government schools. Relevant organisations can adopt appropriate information security and network security measures based on business needs.

After the promulgation of the Guidelines in April, the DPO has arranged a number of briefing sessions to introduce the requirements of the Guidelines and technical solutions to B/Ds, and has provided technical advice to

facilitate B/Ds' compliance with the requirements of the Guidelines and formulation of the corresponding implementation plans within six months.

The DPO will continue to provide appropriate support to B/Ds, including arranging more briefing sessions and sharing technology solutions, and work together to safeguard the government information system and network security.