PCPD
H K
PCPD.org.hk
Guidance Note
香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

# Protecting Personal Data under Work-from-Home Arrangements: Guidance for Organisations

## Introduction

1. Work-from-home (WFH) arrangements have been made from time to time during the COVID-19 pandemic. Under WFH arrangements, organisations may have to access or transfer data and documents through employees' home networks and employees' own devices, which are less secure than the professionally managed corporate networks and devices. This inevitably increases risks to data security and personal data privacy.

2. This Guidance serves to provide practical advice to organisations (including business entities) to enhance data security and the protection of personal data privacy under WFH arrangements.

## General principles for WFH arrangements

3. Regardless of whether one works in the office or works from home, the same standard should apply to the security of personal data and the protection of personal data privacy. Organisations that implement WFH arrangements should adhere to the following principles:

(1) setting out clear policies on the handling of data (including personal data) during WFH arrangements[1] ; and

(2) taking all reasonably practicable steps to ensure the security of data, in particular when information and communications technology is used to facilitate WFH arrangements, or when data and documents are transferred to employees[2].

1 Data Protection Principle (DPP) 5 in Schedule 1 to the Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong)
2 DPP 4

## Practical advice to organisations

4. Organisations, as data users and employers, are primarily responsible for safeguarding the security of personal data and protecting their employees' personal data privacy. The following measures should be implemented by organisations in order to give effect to the general principles for WFH arrangements.

### *Risk assessment*

5. WFH arrangements may be unprecedented or new to many organisations. Organisations should therefore assess the risks on data security and employees' personal data privacy in order to formulate appropriate safeguards.

### *Policies and guidance*

6. In light of the results of risk assessment, organisations should review their existing policies and practices, make necessary adjustments and provide sufficient guidance to their employees. Such policies and guidance may cover the following areas:

   (1) transfer of data and documents out of the organisations' premises and corporate networks;

   (2) remote access to the corporate networks and data;

   (3) erasure and destruction of unnecessary data and materials; and

   (4) handling of data breach incidents.

### *Staff training and support*

7. Organisations should provide sufficient training and support to their employees for WFH arrangements to ensure data security. Training and support may cover the following areas:

   (1) data security techniques such as password management, use of encryption and secure use of Wi-Fi; and

   (2) awareness about cybersecurity threats and trends, such as phishing, malware and telephone scams.

8. Organisations should deploy designated staff to answer questions from employees and provide necessary support.

### *Device management*

9. Organisations may provide their employees with electronic devices (such as smartphones and notebook computers) under WFH arrangements. The following steps should be taken to ensure the security of the data, including personal data, stored in the electronic devices-

(1) installing proper anti-malware software, firewalls and the latest security patches in the devices;

(2) performing regular system updates for the devices;

(3) ensuring that all work-related information in the devices are encrypted;

(4) setting up strong access controls, such as requiring the use of strong passwords (with a combination of letters, numbers, and symbols), requiring changing of passwords regularly and using multi-factor authentication; limiting the number of failed log-in attempts;

(5) preventing the transfer of data from corporate devices to personal devices;

(6) enabling remote wipe function so that information in the devices can be erased if the devices are lost; and

(7) avoid putting the names, logos and other identifiers of the organisations on the devices conspicuously to avoid unwarranted attention.

***Virtual Private Network (VPN)***

10. VPN is an important and popular tool for WFH arrangements because it enables employees to access corporate networks remotely and more securely via the internet. Organisations should ensure the security of VPN by, for example:

(1) using multi-factor authentication for connecting to the VPN;

(2) keeping security setting of the VPN platform up-to-date;

(3) using handshake protocol (such as Internet Protocol Security (IPSec), Secure Socket Layers (SSL), Transport Layer Security (TLS), etc.) for establishing secure communication channels between employees' devices and the corporate networks;

(4) using full-tunnel VPN where possible (using split-tunnel VPN only when necessary, such as in circumstances of insufficient bandwidth); and

(5) blocking the connection from insecure devices.

### *Remote access*

11. In addition to using VPN, organisations should implement further security measures for remote access to their corporate networks. Practicable measures include-

    (1) implementing network segmentation to divide a network into multiple segments or subnets, thereby reducing the risk and magnitude of data breach incidents as well as enhancing the protection for critical and sensitive data;

    (2) granting assess rights to employees on a need basis, for instance, using role-based access control;

    (3) enabling account lockout function to prevent login by a user after multiple failed login attempts; and

    (4) reviewing logs of remote access to identify any suspicious activities.


香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

PCPD.org.hk

PCPD website

Download this publication

**Enquiry Hotline :** **(852) 2827 2827**
**Fax :** **(852) 2877 7026**
**Address :** **Room 1303, 13/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong**
**Email :** **communications@pcpd.org.hk**





First published in November 2020