LC Lawyers
林朱律師事務所
Law firm member of the
EY global network

Work from home arrangements and data security

Rossana Chu / Jacky Chan

26 March 2021

Work-from-home (WFH) arrangements are quite common during the COVID-19 pandemic. Under the WFH arrangements, organizations and employees are often accessing or transferring data and documents through home networks and personal devices that are less secure than the professionally managed corporate networks and devices - thereby increasing risks to data security and personal data privacy. In this article, we explore practical ways that organizations and employees may manage such risks.

Provide sufficient guidance and training to employees

For many organizations, WFH arrangements are something new and therefore should assess the risks on data security and employees' personal data privacy in order to formulate appropriate safeguards. Such assessment may start with a careful review of the existing policies and practices on the following areas:

(1) transfer of data and documents out of the organizations' 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.

Further, organizations should allocate resources to answer WFH questions from employees and provide sufficient training and support regarding (i) data security techniques, e.g., password management, use of encryption and secure use of Wi-Fi; and (ii) awareness about cybersecurity threats and trends, e.g., phishing, malware and telephone scams.

WFH principles to follow

Employees should follow their employers' policies on the handling of data (including personal data) and take reasonably practicable steps to ensure the security of data, in particular when information and communications technology is used to facilitate WFH arrangements, or when the data and documents are transferred during WFH periods.

The following steps should be taken by employees to ensure data security when they have to remotely access their employers' corporate networks during a WFH period

and/or bring electronic and paper documents home for work:

(1) setting strong passwords, changing the passwords regularly and not sharing the passwords with other devices and accounts;

(2) not inserting personal devices (i.e., personal USB flash drive) into corporate devices because personal devices may be prone to containing malware or other security vulnerabilities;

(3) encrypting the data if portable storage devices are used for transferring or storing data;

(4) not sharing corporate devices or documents with family members;

(5) turning off or locking the devices when they are not in use; and

(6) promptly reporting any loss of corporate devices to employers.

Public Spaces and Wi-Fi

In general, employees should avoid working in public places to prevent accidental disclosure of personal data or confidential information to third parties. However, if this is unavoidable, then screen filters should be used to protect information displayed on the screens of electronic devices.

Using public Wi-Fi for work purpose should be avoided. Employees may use the hotspot sharing function of their mobile phones if internet connection is needed for other devices for work. The following steps should also be considered to enhance the security of the connection when using Wi-Fi:

(1) adopting up-to-date security protocol (i.e., Wi-Fi Protected Access 3 (WPA3) or Wi-Fi Protected Access 2 (WPA2)) to encrypt the data in transit and safeguard against attacks);

(2) not using the default login names and passwords of the Wi-Fi routers;

(3) setting strong passwords for the Wi-Fi networks and changing the passwords regularly;

(4) updating the firmware of the Wi-Fi routers in a timely manner; and

(5) reviewing the devices connected to the Wi-Fi networks regularly to identify and remove suspicious devices.

Electronic communications and paper documents

To ensure security of electronic communications, employees should:

(1) avoid using personal email accounts or personal instant messaging applications for work;

(2) use only corporate email accounts for sending and receiving work-related documents and information;

(3) encrypt emails and/or attachments if they contain personal data or restricted information;

(4) double-check the names of recipients carefully before sending emails and instant messages, especially when the emails or the messages contain personal data or restricted information; and

(5) beware of phishing and malicious emails; do not open suspicious links or attachments; verify the genuineness of suspicious emails and messages

with the senders by other channels, e.g., by telephone.

If it is necessary for employees to bring paper documents home for work, the following steps should be taken:

(1) seeking approval from supervisors;

(2) redacting or removing personal data, restricted information and other unnecessary information from the paper documents before leaving office, where practicable;

(3) keeping a register of paper documents that have been taken home;

(4) taking extra care of the paper documents when travelling;

(5) locking paper documents in a secure cabinet or drawer at home to prevent unauthorized access;

(6) returning the paper documents to offices as soon as possible when they are no longer necessary to be kept at home; and

(7) not disposing of work documents with personal data or restricted information at home. They should be shredded in accordance with the established procedures in the office.

Video conferencing

During the COVID-19 pandemic, video conferencing has fast become the new normal. Nevertheless, the increasingly prevalent use of video conferencing software can create new risks to data security and personal data privacy.

Organizations should review and assess the policies and measures on data security and personal data privacy in respect of different video conferencing software and applications, in order to choose the ones which meet their requirements. The following standard security measures should also be adopted:

(1) safeguard their user accounts by setting up strong passwords, changing the passwords regularly, and activating multi-factor authentication, if available;

(2) ensure that the video conferencing software is up-to-date and the latest security patches have been installed; and

(3) use reliable and secure internet connection for conducting video conferencing.

The host of the conference should:

(1) set up a unique meeting ID as well as a strong and unique password for the conference; and provide the meeting ID and the passwords to the intended participants only, and through different means (e.g., email and instant messaging), whenever possible;

(2) where possible, arrange one more "host" (in addition to the main host who is chairing the meeting) to deal with administrative, technical and other contingent issues during the video conference;

(3) set up a virtual waiting room and validate participants' identities before allowing them to join the conference;

(4) "lock" the meeting when all participants have been admitted to prevent unauthorized access;

(5) only allow those participants who need to make presentations to share their screens or documents;

(6) inform all participants and obtain their consents before recording the conference; and prohibit participants from recording the conference; and

(7) store the records of the conference (e.g., video recording and chat messages) securely (e.g., by using password protection or encryption); and delete the records when they are no longer necessary.

Meanwhile, participants of a video conference should protect their personal data privacy by:

(1) being aware of their backgrounds, which may be captured by their cameras and may reveal their personal or sensitive information to other participants; and use virtual backgrounds if necessary;

(2) turn off the microphones (or even the cameras) when they are not speaking;

(3) avoid discussing personal or sensitive information during the video conference as far as practicable; and

(4) close unnecessary documents and windows (e.g. windows showing email, Word documents carrying confidential information) before the sharing of screen to avoid disclosing sensitive information to other participants.

Takeaway

Organizations and its employees should be mindful of data security issues and personal data privacy risks during WFH periods, as much as they should when they are in their workplaces.

KEY CONTACTS

Rossana Chu
Managing partner
Rossana.Chu@eylaw.com.hk
+852 2629 1768

Jacky Chan
Associate
Jacky-ch.Chan @eylaw.com.hk
+852 2675 2167

Contact us

LC Lawyers LLP
Suite 3106,
31/F One Taikoo Place,
979 King's Road,
Quarry Bay, Hong Kong
Tel: (852) 2629 3200
Fax: (852) 2956 1980
https://www.eylaw.com.hk/en_hk

Follow us on WeChat