SECURITY

Software updates and patches: Ensure that you are able to apply security updates and patches remotely or consider mitigating options.

Central document system: Remind staff to save documents to a central or shared document system to avoid loss of data.

Secure connection: VPN (virtual private network) access to the work environment can be one of the most secure ways of allowing remote working.

Clear communication and policies: Review and, if necessary, revise security policies and procedures to account for increased remote working and ensure that those policies and procedures provide staff with appropriate guidance.

Key contact: Ensure that staff are aware of who they need to contact in case of issues or potential breaches of security.

Phishing: Remind staff of the risk of phishing or other similar scams. There has been an increase in phishing attacks recently as attackers look to exploit the current situation.

Encryption: Make use of encryption tools where appropriate.

Multi-factor authentication: Consider using multi-factor authentication procedures to allow remote access.

Scanning and testing: Continue vulnerability scanning and penetration testing. Security is an ongoing obligation.

Refresher training: Remind staff of their obligations and applicable policies regarding security and data protection and consider implementing an online refresher training session.

Asset lists: Track assets given to staff to facilitate home working to ensure that you have a record of assets given out which may hold or allow access to personal data or confidential information.

Dechert LLP