Coronavirus: Home Working Guidance

The Covid-19 (Coronavirus) outbreak is having a major impact on businesses this quarter and, by all accounts, is set to be a major challenge for enterprise throughout the rest of the financial year. At present, there is no advice to ban large groupings or change working patterns however employees with even slight symptoms or a consistent cough should be encouraged to self-isolate for a minimum of 7 days and work from home where possible.

As a result of this it would be beneficial to companies to prepare the information technology and infrastructure needed to support multiple employees working from home. Many companies have already taken steps and pre-emptively instructed all employees to work remotely where possible.

In providing the infrastructure and support for large-scale home working, organisations need to prepare themselves and their employees for the increased cyber security risks such a shift can bring.

Avoid Staff Isolation

To avoid isolation and make sure you are considering the practicalities of remote working we recommend you consider your home working policy, how you will communicate with staff, how you maintain the sense of team and how employees can continue to maintain contact with their colleagues.
Some ideas are:

- **Daily team huddle**: start each morning with a catch-up with your team, either by a conference call or video. Ensure the meetings have a set start and finish time, allow a different team member to host each time so everyone is involved.
- **Embrace video calling:** this can replicate the in-person conversations you would normally have in the office and keeps the connections within your team.
- **Keep 121 and team meeting times**: maintain a sense of structure and framework.
- **Stay focussed:** review your goals and KPIs as you usually would. It's important to keep focus on day to day activities. Don't forget about professional development topics and company values too. Encourage people to share any "need to knows" or challenges so others can help where possible.
- **Virtual drop-in hours:** you can set up a virtual office through video conferencing platforms which will allow people to drop in and out and have live conversations with you. If video conferencing isn't available, then ensure employees are aware of other methods of communication.
- **Schedule team time:** remote workers need time to bond with their colleagues. To replace the chat they would have in the office you can host a standing time each day or week for staff to blow off steam. Encourage them to text and chat about what's happening throughout the day on a team feed and celebrate wins.
- **Dress the part:** remind staff it is business as usual and that they should be ready to jump on any last-minute video calls.
- **Share Calendars:** remind staff to keep managers/team up to date with their availability, even if it's to step away to grab lunch.
- **Have a professional, clear working space:** to be productive it's best to have a clear, dedicated are to work. Take data protection and GDPR into and ensure data is stored and destroyed as per policy. Respect family needs and be mindful not to allow work to encroach on family time.
- **End of day ritual:** The commute home offers a transition from a work to a home mindset. If already home, it's helpful to have a specific activity to signal the end of the workday. This could be to go for a walk with the dog, play with the kids, or cook a meal.
- **Keep a work life balance:** staff still need to take a break from their screens to recharge. When working remotely it can be easy to plough on, help staff to set boundaries between work and home.
- **Look after energy levels:** it is a scientific fact that stress and tiredness suppress immune systems and make us more vulnerable to colds and viruses. So, in addition to physical common sense strategies such as exercising, sleep and eating a balanced diet encourage your staff to remain calm and stay connected.

Data and device security

To ensure your data is as safe as it would be in the office:

- **Use full disk encryption** so if a machine is lost the data isn't accessible to thieves.
- **Remind employees to log out** when they're not using the system.
- **Robust password management** for laptops where all accounts require unique login credentials.
- **Basic security procedures** may need to be reiterated to staff (such as not leaving property unattended in public)

There is a higher risk of data leakage and unauthorised access when connecting with corporate networks remotely. As they're in a relaxed setting, employees may engage in behaviour they wouldn't at the office, such as using a device for personal activities. Home and public WiFi services present attack opportunities outside of the control of your IT security team.

To combat this:

- A VPN can be used to connect remotely to enterprise networks and servers. This is a virtual private network which works as if the device were connected to the organisations LAN, with encrypted communications.
- Do you have a policy about use for company devices for personal use? If so staff should be advised that any non-work activity should be conducted on their own devices.

Whether they're based in-house or remotely employees are open to phishing campaigns. However, with different surroundings to normal and being 'home alone' employees may be receiving increased email communications. This can make it more difficult for them to identify what is or isn't a scam.

To help your staff understand the risks:

- Train them to habitually inspect links before clicking by hovering over them with the pointer to see the actual URL destination.
- Train them to deny requests to enable Macros when opening email attachments.

For more information and for a sample home working policy please contact the Crown Safety Team info@crown-safety.co.uk or call us on 01506 858 858.