equilibrium risk
security & risk management

# Cyber Security
# Remote Working Checklist

# Remote Working Checklist

Thank you for downloading this Remote Working Checklist. We have teamed up with the Cyber Management Alliance to provide this document. It is by no means a comprehensive list, but we do hope you find it useful and it helps you be more prepared for cyber security attacks. Remember you can always get in touch with us if you need any specific advice.

| **Cybersecurity** | **Check** |
|---|---|
| Remind staff about the need to protect confidentiality | |
| Remind staff **NOT to lend** their machines to their children or other members of the family | |
| Remind staff that you are **MONITORING** their activity as per your policies and terms and conditions of employment | |
| **Update of software and OS:** Ask staff to keep their devices (corporate and personal) fully updated | |
| **Provide a VPN** and or remote working solution for your staff (ensure you validate the VPN solution) | |
| Send out regular reminders about **critical software and mobile update** (eg: Adobe, Apple, Android, Chrome, Firefox) and ask staff to update (show them how using recorded screencasts if necessary) | |
| **Disable email forwarding** for all accounts OR setup and alert if email forwarding is switched on | |
| **Passwords** | |
| Staff **MUST not share** passwords via email or SMS messages (where necessary, phone the other party. | |
| Ask staff to use password managers (a very strong password for the password vault, written down and stored safely) | |
| Remind staff that you will NOT call them about password resets (to help avoid being scammed) | |
| Make 2 factor authentication (2FA) mandatory for all remote workers | |
| Including email when accessing any critical systems or applications | |
| Ensure you have BACKUP CODES in case 2FA does not work | |
| Use an APP for 2FA rather than SMS (free apps include Google's authenticator) | |
| Store these backup codes safely, preferably in a locked safe | |
| Ensure you know how to backup and restore 2FA tokens you are using (eg: Google Authenticator etc) | |
| **Mobile Equipment** (Remember, these are now critical devices and must be treated as such) | |
| Ensure all your mobile equipment has **hardware encryption** (where not possible, software encryption is OK) | |
| All mobile devices must have FULL disk **encryption** | |
| If you are renting laptops/desktops, please ensure that you **WIPE the hard disks** to ensure no residual data is left behind. This MUST be on top of you to-do-lit when things go back to normal OR when you have to return your machines | |
| Where staff are using personal devices, remind them **not to download Apps** from non-trusted sources. They are HIGHLY likely to contain malware. | |
| Mobile devices are now **business critical** machines and must be subject to the same stringent policies as software updating, backup and protective controls | |
| Keep extra stock of mobiles, laptops, microphones, and other peripherals | |
| If possible, use Google's DNS servers or CISCO's umbrella DNS and force all laptops and mobile devices to use these. Advise staff to do the same on their personal devices (if unsure, ask for external help) | |
| **Privileged Users (Hold the keys to the kingdom)** | **Check** |

| | |
|---|---|
| Ensure you inform all IT and business privileged users: | |
| Remind them of their responsibilities | |
| Insist that they DO NOT login for DAILY tasks with high privileges | |
| Demand that they REPORT all errors/ confess to mistakes immediately | |
| Ensure they use 2 factor authentication at all times. No exceptions | |
| Ensure that NO procedures are bypassed (no emergency change without approval etc) | |
| **Phishing Emails and Scams** | |
| Remind staff **NOT** to open links or documents with Coronavirus information. Ask them to report these | |
| Remind staff that it's **OK to make a mistake** and that they should own up if they have: | |
| Accidentally clicked on a suspicious link | |
| Opened a suspicious PDF or Word, excel file with a macro | |
| Staff **MUST** report malware/ ransomware infections immediately | |
| Caution staff about **remote helpdesk calls** purporting to be from Microsoft or other computer vendors | |
| Remind staff to be cautious about pop-ups about VIRUS warnings when surfing the web | |
| **Important Communications:** If relevant, remind staff that critical emails only come from a specific email OR the CEO never sends email from his personal account | |
| **Policy and Illegal Activity** | |
| Take this opportunity to remind users about your AUP or Acceptable Usage Policy (or other policies) | |
| Remind staff that surfing porn sites on corporate machines, amongst other things, is illegal | |
| Remind staff that using corporate devices to entice hatred, research terrorist related activities, is illegal: | |
| IT staff must be reminded | |
| NOT to use corporate machines to run hacking tools | |
| NOT to attempt illegal activities (like attempting malicious hacking, scanning etc)on office time OR using any other corporate resources | |
| Staff must be conscious of the **employer's reputation** when tweeting social messages on Twitter, LinkedIn etc. | |
| Remind staff they **MUST not use** unapproved USB flash drives and unapproved cloud services | |
| **Working Remotely, Online Meetings & Calls** | |
| Remind staff **NOT** to have confidential calls and business discussions near SMART speakers like Amazon's Alexa, Apple's Homepod and Google's Home | |
| Remind staff to **MUTE** their microphone when they are not speaking in a conference call | |
| Educate all staff to ensure webcams are **blocked** by default (both physically and by the conference app you use) | |
| Remind staff **NOT** to leave their machines unlocked, especially during a call or when visiting the loo, especially in a public place | |
| Ask staff **NOT** to work from coffee shops or public places (if possible) – especially if they are on confidential calls or working in confidential documents | |
| Request staff NOT to use **'Print to email'** offered by printers | |
| **'Buddy up'** with a colleague & swap mobile numbers and check in each morning | |
| If possible, ask that screen savers be used to make shoulder-surfing harder | |
| Ask staff **NOT to use just ay VPN** solutions to ace corporate resources. This is quite important as VPNs are recommended to stop snooping and interception. However, **several VPN software's are malicious** | |
| Staff **MUST not** switch on forwarding of corporate emails to their personal emails AND/ OR must not use alternative email clients to access corporate email. | |

| | |
|---|---|
| **Exceptions & Change** (Get ready to grant exceptions left, right and centre) | |
| If you don't have one yet, create an 'exceptions' register | |
| Create a review-by-date and put multiple calendar reminders for you/ your team to review them | |
| Where possible, have a 'no way this is an exception' list | |
| Pay special attention to change management and carry out a weekly or monthly review | |
| **Privacy** | |
| Remind all staff of their responsibility to **respect** the privacy of your clients and staff | |
| Remind IT and cybersecurity folk to be extra vigilant for possible malicious activity on user accounts | |
| Ask staff **NOT to PRINT** personal information | |
| Staff must be reminder **NOT** to email personal information via email OR store personal information in non-approved locations | |
| Staff members may be exchanging personal phone numbers and/ or emails. If possible, avoid this OR ask staff to prepend **'delete-later'** to the name of staff if they save these details | |
| **Cyber Attack & Incident Response** | |
| Constantly remind staff to be on alert for phishing emails and other attempts to compromise/ steal account details | |
| Staff must report all phishing emails and malicious activity | |
| If staff suspect something malicious, encourage them to call certain stakeholders, especially if they do not receive any response via existing channels | |
| Security staff must be **extra vigilant** and actively seek out suspicious activity (given remote working habits of users this may be operationally expensive) | |
| Ask IT and security staff (including outsourcers/ partners) to pick up the phone and call if its important rather than rely on email. Use a **separate out-of-band app** or something as simple as Whatsapp groups for urgent communications | |
| Keep a **printed** copy of your procedures and checklists at home AND make sure they are **notr** easily accessible | |
| **Monitor** endpoints (laptops etc) more closely and if possible, use EDR type tools urgently | |
| **Never too late:** Start working on your Cyber Incident Planning & Response strategy now | |
| **Backup Backup Backup** | |
| Provide staff software to ensure their critical documents are backed up | |
| Ask staff to back up data on an approved external hard disk that is **NOT** permanently connected to the device | |
| Ask staff to use only approved cloud storage services (if permitted) | |
| Encourage staff to reach out to discuss any cloud storage or cloud service solution that they want to use. Cloud services include, but are not limited to:<br>• File sharing services<br>• File storage and synchronisation<br>• Project management apps or services<br>• Collaboration tools and services<br>• Note taking and storage solutions<br>• Photo storage and sharing services | |
| **HR & Mental Health & Occupational Health** | |
| Check that HR have got in place policies to deal with occupational health in a remote working setting. Remote working maybe the norm for a sustained period of time. Practices such as "working from the sofa" can produce other health issues i.e. back problems. Formal policy and risk assessments are strongly recommended | |
| Remind staff that they should reach out to discuss any mental health issues | |

| | |
|---|---|
| Set clear **working-time boundaries.** (Remote working can often lead to unrealistic expectations where the assumption is that staff will be available all the time) | |
| **Enable staff to confidential send** critical messages (health, safety, mental health, security, crisis) quickly and securely. Do this preferably via a mobile app. DO NOT use email please. | |
| **Video & Audio Conferences** | |
| Send out regular reminders to staff about using only officially approved conference apps | |
| Remind staff to read about and be aware of basic security and privacy settings like:<br>• Having a password for every meeting or conference call<br>• Camera must be switched off OR blocked by default, for both the host and attendees<br>• Microphone is on MUTE by default<br>• Kicked out participants CANNOT re-join<br>• Ask staff to ensure their meetings are NOT being recorded<br>• If you are recording please inform all participants<br>• Remind staff to EXIT or close the app once the conference is complete | |
| **Helpdesk & Support** | |
| Support staff must be on high alert and challenge password resets and 'strange' requests | |
| Ensure you review/ audit permissions and privileges of helpdesk staff | |
| If possible, introduce extra user identity verification for all users | |