ASTONLARK

CYBER SECURITY CHECKLIST

There are a number of cyber security considerations for your business as it returns to work.

BEFORE FURLOUGHED STAFF RETURN TO WORK

- ☐ Review access and activity logs for all devices and services, if available, to ensure accounts have not been used, misused or abused during furlough.
- ☐ If colleague accounts have been locked or frozen to prevent access during furlough, now is the time to review access privileges prior to work being resumed.
- ☐ If staff are returning to a workplace with hotdesks, ensure that suitable Health & Safety measures are in place to reduce contamination between colleagues.
- ☐ If you are still using any computers with Windows 7, consider upgrading that equipment if affordable to do so. Windows 7 is no longer supported by Microsoft, and therefore will leave you exposed to security vulnerabilities.

FOR FURLOUGHED STAFF AS THEY RETURN TO WORK

- ☐ Before colleagues make use of any office computer equipment, ensure that all software updates are installed, including operating system updates, and that anti-malware software is up to date and a full scan is undertaken.
- ☐ If colleagues have made use of personal devices while working remotely, and there is no longer the need, ensure the device is cleaned of all business information, including documents and saved passwords.

IF FURLOUGHED STAFF WILL NOT BE RETURNING TO WORK

- ☐ Ensure that all company-owned devices are retrieved as soon as possible.
- ☐ Ensure that accounts used by the ex-colleague are frozen or deleted as soon as possible.
- ☐ Review any licence agreements you have for the services that were in use. You may be overpaying for too many licences.

CONSIDER SERVICES TAKEN UP DURING REMOTE WORKING

- ☐ If colleagues will no longer be working remotely, ensure any service accounts or access privileges granted to enable remote working are removed or deleted.

CONSIDER THE FUTURE

- ☐ Business is likely to be affected until there is a viable vaccine for Covid-19. As such, you will likely be considering entrenching or investing in new means of working driven by technology solutions. Ensure that security and data protection are considered when assessing such projects.
- ☐ Covid-19 has highlighted the necessity for trust in our IT infrastructure, internally and in our supply chains. Cyber assurance certifications are available to evidence investment in cyber security.

AL-RM-022-0520

Chartered Insurance Brokers