Cybersecurity Checklist

List	Check
User Awareness	
Procedures for password reset and remote support.	
Encourage staff to use password managers.	
Remind staff to be careful with unknown emails, and if they are not sure, it's better to report and ask for guidance.	
Mark all the emails that are not internal as "EXTERNAL" this way, fake email that claims to be internal should be easy to identify.	
Remind staff about the need to protect confidentiality.	
Ask staff NOT to defer critical updates to the software.	
Staff must not visit sites like illegal movie websites, porn, gambling etc. as they pose a risk of ransomware and malware infection.	
Remind staff NOT to lend their machines to their children or other members of the family.	
Stress the IMPORTANCE of NOT sharing passwords (remote working can lead to more password sharing).	
Remind staff that it's okay to make a mistake and that they should own up if they have: - Accidentally clicked on a suspicious file and/or link - Opened a suspicious PDF or Word, excel file.	
Staff MUST report malware/ransomware infections immediately they notice it.	
If not working from home, where possible, ask that screen filters are used to make shoulder-surfing harder.	
Remind staff not to connect to unsecured and unknow WI-FI networks or public WIFI.	

List	Check
Online Meetings and calls	
Remind staff to MUTE the microphone when they are not speaking in a conference call.	
When creating a new meeting, always make sure they are password protected.	
Educate all staff to check webcams are on or off when they start a call of Teams, Zoom, WebEx etc.	
Remind staff NOT to leave their machines UNLOCKED, especially during a call or when visiting the restroom?	
Educate staff to make sure they know everyone in the meeting, and there are no unknown phone numbers or people on the call.	
Ask staff NOT to work from coffee shops or public places (if possible) – especially if they are on confidential calls or working on confidential documents.	
Remind staff to dress appropriately for video calls.	
Remind staff to not have any confidential information on the background during video calls.	

List	Check
Laptops and End-User Devices	
Ensure laptops/devices use native hard drive encryption where possible.	
Ensure laptops/devices have Endpoint Protection/Antivirus Installed on the devices.	
Ask staff not to buy or use unknown or suspicious USB or Bluetooth vendors with their devices.	
Ask staff not to use their laptops USB ports as charging station for home or any other devices.	
Ensure software distribution technology can distribute software to devices, not on corporate networks.	