Cyber Basics Review (CBR)

To be completed in conjunction with the CBR Information Pack.

SECTION 1 - FIREWALLS	Y	N
1. Do you have a firewall(s) installed and switched on across your boundary and devices?		
2. Does your firewall(s) monitor both traffic coming in to and leaving your network?		
3. Have all default passwords been changed to one that is individual, unique and secure? *Password guidance can be found by searching 'password' on https://www.ncsc.gov.uk*		
4. Are firewall updates automatically enabled and scheduled?		
5. Have all rules and exceptions from trusted websites been set to 'allow' and reviewed to ensure they are still relevant?		
SECTION 2 – SECURE CONFIGURATION	**Y**	**N**
1. Does each system or application have an individual password that is secure and changed from the default setting?		
2. Is there a password policy in place that includes password/account lockout, re-use and resetting?		
3. Are default or no longer supported software and applications removed if they are not required?		
4. Are devices configured NOT to auto-run or auto-play?		
5. Are any Wi-Fi networks password protected (changed from default passwords)? (Consider switching SSID broadcast off)		
SECTION 3 – PATCH MANAGEMENT	**Y**	**N**
1. Are all operating systems, apps and firmware running legitimate and licenced software?		
2. Are all operating systems, apps and firmware regularly updated and patches applied?		
3. Are all critical or high risk patches applied within 14 days of being released?		
4. Are all devices (including PC's laptops, tablets and mobile devices) set to log off but not shut down at the end of the day to allow updates to be applied remotely?		
5. Have you considered legacy planning for all operating systems and software where it is known it is coming to its end of life?		
SECTION 4 – ACCESS CONTROL AND ADMINISTRATION	**Y**	**N**
1. Is there a dedicated person/party who look after your IT? This can include outsourced IT companies).		
2. To prevent unauthorised access, are accounts with administrative access only used for administrative tasks? I.e are standard user accounts used for day to day tasks?		
3. Are you following the principle of least privilege for user access with an appropriate policy for reviewing and revoking of access to user accounts?		
4. Does each individual user have an individual user name and password for accessing the network?		
5. Is 2FA (Two Factor Authentication) used where possible and practical?		
SECTION 5 – MALWARE PROTECTION	**Y**	**N**
1. Are all of your computers, laptops, tablets and mobile devices protected from malware by having individual anti-malware installed?		
2. Is your anti-malware software configured to:		
• Scan files automatically upon access?		
• Scan webpages automatically when access through a web browser?		
• Prevent connections to malicious websites on the internet?		
3. Does your network limit the installation of applications to an approved set (i.e. using an App Store or application whitelisting)?		
4. Does your network connected device use application sandboxing (i.e. by using a virtual machine)?		
5. If applicable, is your software set to open unknown documents in protected mode?		