Cyber Essentials Checklist

Compliance with this checklist will achieve alignment with gov.uk cyber essentials recommendations.

Firewall

- Do you have a Boundary Firewall in place to protect the network in Scope?
- Have all default passwords for the firewall(s) been replaced with strong passwords and have all open ports been checked and approved by a qualified and authorised business representative?
- Have you ensured that all commonly attacked and vulnerable services are blocked or disabled at the boundary firewalls?
- Do you have a policy in place to remove any unnecessary firewall rules and do you have any open ports or services which are not essential to your business?
- Do you disable or remove all remote administrative interfaces on your firewall devices?
- Are your firewalls configured to deny access to the internet by default and if so, is this effective?

Devices

- Are all unnecessary or default user accounts disabled on your devices?
- Do all your accounts have strong passwords where the default password been changed?
- Have you disabled or removed all unnecessary software, Auto Run or any similar services for all media types and network file shares?
- Have you installed a host-based firewall on all desktop and laptop computers which block unapproved connections by a device?
- Do you use a standard build process to commission each new device in order to ensure it is built in line with security requirements, and is this process kept up-to-date in with your corporate policies?

Backups

- Do you have a backup policy in place to protect your systems, creating backups at agreed interval?
- Do you have more than a single back up mechanism?

Event logs

- Are security and event logs maintained on your servers and does this extend to desktop and laptop computers?

User Accounts

- Do you follow an agreed approval process before authorising user account requests, and do you ensure these accounts are assigned to named individuals?
- Do users authenticate with a unique user name and strong password to gain access? Are all user accounts disabled or removed when no longer required?

Administrator Accounts

- Do you restrict special access privileges such as administrator accounts to a number of authorised individuals, and keep a records of these privileges to review every three months?
- Do you withhold internet and email permissions for all activity on your administrative accounts?
- Do you have a password policy in place and are all administrator passwords replaced every 60 days to a complex password?

Malware Protection

- Do you have malware protection software installed on all computers that can connect outside of your scope network and a policy in place requiring updates to the software are applied within 90 days?
- Are all anti-malware signature files kept up to date and is the software configured to scan files upon access and scan files downloaded from the internet or removable/ remote storage systems before they're accessed?
- Does the software scan websites for malicious content, and do you have a policy in place to prevent the access of malicious websites?
- Does the software run at least daily scans of your systems?
- Do you have access control measures in place in addition to anti-malware definition files

Software Installation and Patches

- Is all software installed on computers and network devices licensed, and is this software supported?
- Are all security patches for your Operating System applied within 14 days of release?
- Is all legacy or unsupported software removed or disabled from your devices?
- Do you have a policy to ensure all mobile devices are maintained with vendor updates and app patches?