THE CYBER RESILIENCE CENTRE FOR THE WEST MIDLANDS

Cyber Security Checklist

- [ ] **Use strong passwords:** Passwords should be difficult to guess – it's best to avoid obvious passwords that use personal information like birthdates as a hacker could obtain such information. Many web browsers now have built-in secure password generators which takes the guesswork out.

- [ ] **Use current firewall and anti-virus software:** Firewalls are designed to minimise the amount of harmful traffic reaching your devices. Be sure to regularly update the software that you use so that these can defend against emerging threats.

- [ ] **Train staff on cyber security best practices:** All employees that have access to or use online information pertaining to your business should be trained on how to manage this data and awareness on managing cyber security threats.

- [ ] **Routinely back up data/files:** In the event of a security breach, your data is vulnerable to corruption or deletion which can disrupt business continuity. You may be at risk of losing important designs, contracts or project information that destabilises operations.

- [ ] **Install patches and updates:** Software developers provide ongoing support in the form of patches and updates, which will fix any system security vulnerabilities as they appear. However, older operating systems and software won't receive this support, so make sure you're using the latest versions and that your software is still supported.

- [ ] **Conduct a cyber security risk assessment:** Help identify any potential vulnerabilities or gaps in your security, like would with a physical job site. The risk assessment will also highlight areas where improvements are needed.