

# CYBER-SECURITY SMALL BUSINESS CHECKLIST

This checklist is based on the 5 Steps to Cyber-Security for Small Businesses and Charities. Complete these simple and low-cost measures to improve your organisation's cyber security posture.

## Policy Actions

Staff members responsible for determining the overall cyber-security policy should carry out the following actions:

- Identify and record essential data for regular backups.
- Create a password policy – Information about creating password policies can be found on the UK National Cyber-Security Centre's website, <https://www.ncsc.gov.uk/collection/passwords/updating-your-approach>
- Decide what access controls your users need so they can access only the information and systems required for their job role.
- Decide what staff need access to USB drives or other portable storage mediums, e.g. CD's.
- Relevant staff members should sign up to threat alerts and stay up to date with local cyber-security related news and reports.
- If USB's are required, create an inventory of approved USB drives and their owners, and review whether ownership is necessary periodically.

## Technical Actions

Staff members responsible for the setup and configurations of devices, networks and software should carry out the following actions:

- Switch on your firewall.
- Install and turn on anti-virus software.
- Block access to physical ports and drives for staff who do not need them, e.g. USB ports, CD drives.
- Ensure data is being backed up regularly to a backup platform, e.g. external hard drive and/or the cloud.
- Set automated backup periods relevant to the needs of the business.
- Switch on password protection for all available devices, and change default passwords on all internet-enabled devices in line with the password policy.
- Install and turn on tracking and remote wiping applications for all available devices, e.g. Find My iPhone.
- Consider providing access to an approved password manager for your staff to secure their passwords.
- Enable multi-factor authentication (MFA/2FA) for all important accounts, e.g. email.
- Keep software, hardware and devices up to date.

- Switch on automatic updates for all devices and applications where possible.
- Use encryption on computer systems and devices where available. Microsoft Windows provides an encryption feature called BitLocker (may require a Trusted Platform Module (TPM)), and Apple Mac OS uses FileVault.

## Training and Awareness Actions

Staff responsible for implementing staff training and awareness should carry out the following actions:

- Provide secure physical storage (e.g. a locked cupboard) for staff members to write down and store passwords.
- Create and implement a cyber-security training plan that can be used for all staff.
- Overview the password policy and explain how to make unpredictable passwords to staff.
- Include how to spot the obvious signs of phishing.
- Staff should be made aware of the reporting process for incidents and suspected phishing attacks.
- Provide staff with details on how the business operates and how they deal with requests via email.
- Make staff aware of Wi-Fi hotspot vulnerabilities and how to use alternative options.

For more information about the actions in this checklist, look for the '5 Steps to Cyber-Security' section in our [OCSIA Knowledge Base](#).

If you have any concerns, or have been affected by a cyber-related issue, report it to the Office of Cyber-Security and Information Assurance (OCSIA) by submitting a Cyber Concerns Online Reporting Form at [www.gov.im/ocsia](http://www.gov.im/ocsia).