CYBER ESSENTIALS

REQUIREMENTS UPDATE

CLOUD SERVICES

Cloud services are to be fully integrated into the 2022 update.

There is a commonly held assumption that cloud services are secure by default - this is incorrect. Organisations are now responsible for all Cyber Essentials controls and applying these, where possible.

MULTI-FACTOR AUTHENTICATION

Due to the rise of attacks on cloud services, multi-factor authentication must now be used to provide additional protection when connecting to cloud services.

MFA requires users to supply multiple credentials before being able to access an account.

HOME WORKING

Any devices used by remote workers to gain access to organisational information, whether they are owned by the organisation or not, are now in scope for Cyber Essentials.

The use of (single tunnel) Virtual Private Network (VPN) transfers the boundary to the corporate firewall or virtual cloud firewall.

Thin clients (dumb terminal) are also in scope when they connect to organisational information or services.

UNSUPPORTED SOFTWARE

All software on in-scope devices must be:

- **Licenced and supported.**
- **Removed from devices when it becomes unsupported.**
- **Have automatic updates enabled, where possible.**
- **Updated within 14 days of an update being released.**

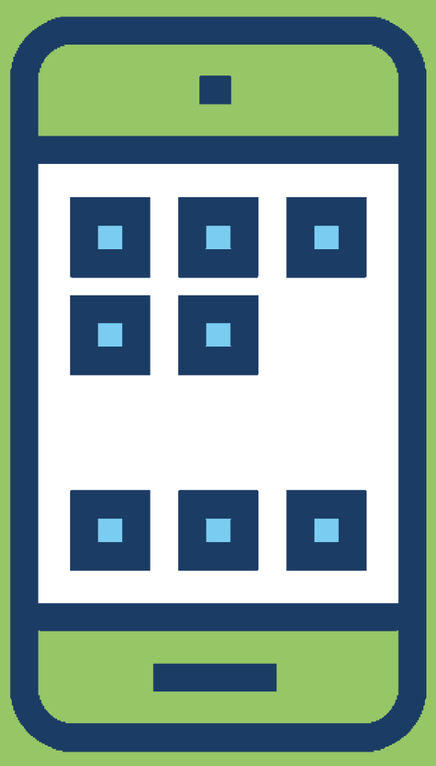
PASSWORDS

When using passwords, one of the following protections must be used:

- **Multi-factor authentication.**
- **Throttling the rate of unsuccessful or guessed attempts.**
- **Locking accounts after no more than 10 unsuccessful attempts.**

Technical controls are used to manage the quality of passwords. This will include one of the following:

- **Using multi-factor authentication in conjunction with a password of at least 8 characters.**
- **A minimum password length of 12 characters.**
- **Using automatic blocking of common passwords, and a password of at least 8 characters.**



SMART DEVICES

All smart phones and tablets connecting to organisational data and services are confirmed in scope when connecting to corporate networks or mobile Internet such as 4G and 5G.

Biometrics or a minimum password/PIN length of 6 characters must be used to unlock a device.

The scope of an organisation must also include end-user devices.

There will a grace period of 12 months to allow organisations make the necessary changes for the following requirements:

- The requirement for MFA will apply for admin accounts from Jan 2022 and the requirement for MFA for users will be marked for compliance from Jan 2023.
- The requirement for support and updates on Thin Clients will be marked for compliance from Jan 2023.
- Unsupported software remove from scope will be marked for compliance from Jan 2023.