National Cyber
Security Centre
a part of GCHQ

Security guidance for iOS and iPadOS

Securing your mobile devices is an essential part of guarding your organisation against a variety of threats which herald primarily from the internet. This guidance summarises how organisations can secure devices powered by the iOS operating system, which include the iPhone, iPod touch and iPad.

This guidance is aimed primarily at large organisations, with a focus on those deploying or managing large IT estates. However, if you only have a few devices to look after, this guidance is still appropriate.

> **Note**: iOS is the operating system which powers the iPhone and iPod Touch. iPadOS is a very similar platform and the security considerations are identical to iOS, so this guide refers to both platforms as **iOS**.

In this guidance:

1. General recommendations

- Decide which iOS devices your organisation will use. iOS devices typically receive software updates for around 5 years after first release. Once a device is vintage or obsolete[1], it no longer receives updates. At this point you should purchase newer devices.
- Devices should be supervised[2] by your organisation to ensure you have the most control over which policies to enforce on your devices.
- If possible, use Apple Business Manager (ABM)[3] to supervise, enrol and provision devices using zero touch enrolment. This prevents users from un-enrolling devices, once deployed. Alternatively, use Apple Configurator[4] to manually supervise devices before provisioning to enable more control.
- Once supervised, iOS devices should be managed using a Mobile Device Management service, to enforce technical controls. Also configure the logging and monitoring capabilities of the MDM.
- Use one of the NCSC's recommended network architectures to enable remote access to enterprise services.
- If a virtual private network (VPN) is required, use the built-in IKEv2 VPN, as this provides a high-performance, always-on mode and strong cryptography.
- Third-party apps for work use ('managed apps') should be approved centrally into an enterprise app catalogue and delivered via MDM, to keep data separate from non-work apps.
- Consider your approach to enabling iCloud accounts[5] on users' devices, using on-device policies to manage specific iCloud features.
- Antivirus and other security software are not normally required on iOS.

[1] https://support.apple.com/en-gb/HT201624

[2] https://support.apple.com/en-us/HT202837

[3] https://support.apple.com/en-gb/guide/apple-business-manager/welcome/web#/apdd344cdd9d

[4] https://support.apple.com/en-gb/apple-configurator

[5] https://support.apple.com/en-gb/HT207689

2. Work applications

Most organisations will want to offer their users a range of productivity and business applications so they can consume, create and collaborate remotely. We recommend the use of the built-in apps where possible (e.g. Mail and Calendar) as this gives you the most flexibility to subsequently open work attachments in any managed third-party applications, as well as optimising usability and performance. It also enables accounts to be managed by MDM[6], minimising administrative overheads.

If you are using third-party apps for work, we recommend using an enterprise application catalogue of approved apps that users can choose to install at will, delivered through MDM. Apps deployed in this way will be 'managed' apps and have access to work data. Apps installed through the App Store will be 'unmanaged' and will not have access to the same data.

We recommend that care is taken with high-privilege applications, such as third-party keyboard apps and network extensions. These types of application might be able to access large amounts of work data, so present a higher risk to your organisation.

3. Device configuration

Once you have chosen your MDM service, architecture and approach to applications, you should then develop a device configuration you can apply to enforce your technical controls.

In particular, you should include policies that manage:

- external interfaces[7], including wired and wireless peripherals (e.g. disabling USB accessories when the device is locked)
- the use of biometrics[8], as well as passcodes and authentication policies[9]
- the iCloud[10] (and other cloud) services that you want to allow
- device OS and application updates, including automatic updates[11]

4. Further reading

- Managing Devices and Corporate Data on iOS[12], Apple (PDF)
- iOS Security[13], Apple (PDF)

[6] https://support.apple.com/en-gb/guide/mdm/welcome/1/web

[7] https://support.apple.com/en-gb/guide/mdm/mdmc622d929c/1/web/1

[8] https://www.ncsc.gov.uk/collection/biometrics

[9] https://www.ncsc.gov.uk/collection/passwords

[10] https://www.apple.com/uk/icloud/

[11] https://support.apple.com/en-gb/HT204204

[12] https://www.apple.com/business/resources/docs/Managing_Devices_and_Corporate_Data_on_iOS.pdf

[13] https://www.apple.com/business/docs/site/iOS_Security_Guide.pdf