Australian Government
Australian Signals Directorate

Security Configuration Guide: Apple iOS 14 Devices

For iPod Touch, iPhone and iPad using iOS 14

First published: February 2021
Last updated: October 2021

cyber.gov.au

Table of contents

Introduction

The Australian Signals Directorate (ASD) has developed this guide to assist Australians to understand the risks of deploying iOS 14 and the security requirements that need to be met to allow iOS 14 to handle classified data. This security configuration guide does not replace the *Information Security Manual* (ISM), however, where a technical conflict arises the most current document shall take priority.

Audience

This guide is for users and administrators of devices running iOS 14. These devices include iPod Touch, iPhone and iPad. Note that although tvOS, watchOS and macOS have many similarities, they have not been subject to evaluation under the Common Criteria or an ASD Cryptographic Evaluation (ACE).

To use this guide, readers should be familiar with basic networking concepts, be an experienced mobile device system administrator and be or have access to an experienced network administrator.

Parts of this guide will make reference to product features that will require the engagement of other software, networking equipment or Mobile Device Management (MDM) vendors. While every effort has been made to ensure content involving any third-party vendor products is correct at the time of writing, organisations should always check with these vendors when planning their system implementation. Note, mention of third-party products is not a specific endorsement of that vendor over another and are used for illustrative purposes only.

Some security configuration instructions within this guide are complex, and if implemented incorrectly could reduce the security of devices, networks or an organisation's overall security posture. These instructions should only be implemented by experienced systems administrators and should be used in conjunction with thorough testing.

Purpose

This guide provides information for Australian organisations on the security of Apple iOS 14 devices sold in Australia, and their risks, which should be considered before they are introduced into an organisation's mobile fleet.

This guide provides a summary of features and associated risks for the Apple iPod Touch, iPhone and iPad running iOS 14. Throughout this guide, devices and combinations of software are referred to as the 'iOS platform'.

The advice in this guide has been written for the use of the iOS platform within Australia. Organisations and individuals seeking to use devices overseas should also refer to the *Travelling With Mobile Devices* publication.

Implementing the settings advised in this guide can significantly reduce system functionality and user experience. Authorising officers are encouraged to consider the balance of user requirements and security, as not all advice may be appropriate for every user, environment or deployment.

Organisations should seek approval from their authorising officer to allow for the formal acceptance of the risks. Refer to the *applying a risk-based approach to cyber security* section of the ISM for more information.

This guide is aligned with the ISM, however, not all ISM guidance can be implemented on the Apple iOS 14 platform. In these cases, risk mitigation measures are provided in the *Advice to authorising officers* section.

Evaluation status

Since April 2014, ASD has endorsed the *Mobile Device Fundamentals Protection Profile* (MDFPP) with specified optional mitigations as a key component in all mobile device evaluations. The MDFPP, as defined by the United States National Information Assurance Partnership (NIAP), outlines the security requirements for a mobile device for use in an enterprise. Earlier versions of iOS have been evaluated against MDFPP, and completed an ASD Cryptographic Evaluation (ACE).

This guide is based on the findings of ASD and provides guidance that must be enforced for **OFFICIAL: Sensitive** and **PROTECTED** deployments. Guidance in this publication will also assist organisations to comply with existing policies when deploying devices at lower classifications.

Under the Common Criteria, iOS 12.2 has undergone evaluation against the Protection Profile for MDFPP version 3.1. Apple has also obtained a broad range of additional certifications for their devices.

General advice

Introduction to mobile device security

In this guide, mobile device security advice centres on the three security tenets of:

- device integrity
- data at rest
- data in transit.

ASD evaluates cryptographic implementations to determine configurations necessary to reduce handling requirements of devices used for processing, storing or communicating classified data. It is each organisation's responsibility to configure devices according to ASD advice, and assess that available cryptographic protections are used appropriately.

Configuration advice regarding device integrity aims to provide a level of protection suitable for classified mobile devices. It assumes malicious actors have physical access to mobile devices while powered on and in a locked state. Configuration advice draws upon an assessment of:

- key hierarchy and architecture
- cryptographic implementation
- operating system architecture
- configuration under typical deployment scenarios.

It is each organisation's responsibility to configure devices according to this advice in order to achieve the desired integrity outcomes.

Configuration advice regarding the protection of data at rest aims to provide a level of protection suitable for or classified data stored on an iOS platform. This advice assumes malicious actors have physical access to devices while they are powered on and in a locked state. Configuration advice draws upon configuration assessments and details of application implementations, including availability of security features.

Configuration advice regarding the protection of data in transit aims to provide a suitable level of protection for classified data traversing a network, while assuming malicious actors are able to intercept this traffic. It is each organisation's responsibility to configure devices according to ASD advice and maintain appropriate Virtual Private Network (VPN) infrastructure to support VPN tunnels, noting such infrastructure is out of scope for this guide.

iOS updates

Apple typically releases a beta version of new major iOS versions in June each year, and the release becomes generally available in September. New iOS devices can only run new versions of iOS, but there is scope for the upgrade of supervised devices to be explicitly controlled.

For organisations with existing or planned iOS deployments, ASD advises:

- Actively test beta versions of iOS under AppleSeed for IT and Developer Preview Programs.
- Upgrade to the latest iOS version. This is consistent with ASD's advice to install the latest versions of software and patch operating system vulnerabilities, as communicated in the ISM and the *Strategies to Mitigate Cyber Security Incidents*.
- Implement any interim guidance contained in ASD documents, such as this guide. In particular, organisations should take note of advice relating to new features and changed functionality introduced by Apple in new iOS versions. This advice is the result of in-house technical testing by ASD, experiences shared by other organisations and based on consultation with the vendor.

Details of new iOS security updates are released concurrently with new iOS versions, addressing vulnerabilities. The Apple security updates webpage contains more information. This information may help organisations quantify the risk posed by not updating.

iOS encryption

The iOS platform uses encryption and data protection measures to secure the hardware, software and data. Details of the encryption and data protection measures can be accessed from Apple's *Platform Security Guide*.

When configured in accordance with ASD guidance, the following classes of data protection are available:

- **Class A**: When the device is locked, data afforded 'Class A' data protection is suitably encrypted and inaccessible (note: there is a 10 second window at device lock before the ephemeral key [cryptographic key that is generated for each new session] is discarded).
- **Class B**: When the device is locked and the file is closed, data afforded 'Class B' data protection is suitably encrypted and inaccessible.
- **Class C**: When the device is turned off, or powered on and a user has not yet authenticated to the device, data afforded 'Class C' data protection is encrypted and inaccessible.
- **Class D**: Data encrypted on the device is afforded 'Class D' data protection. However, the nature of the encryption and key handling means that the data is considered accessible.

ASD recommends that all classified data handled by devices uses Class A data protection. In general, basic iOS functionality that would be used by organisations, such as email, attachment viewing and file storage all use Class A data protection by default.

Emails that are stored on devices are afforded Class A data protection, except in the case where an email is downloading or being received while the device is in a locked state. In this situation, the email and any attachments are afforded Class B data protection, which means the data is encrypted with an ephemeral key that is not generated from user credentials. Once the device is unlocked, and a suitable user credential-derived key is generated, the email and any attachments are then re-encrypted to Class A data protection standard.

Supervised devices

ASD guidance advises that devices handling classified data (**OFFICIAL: Sensitive** and above) be supervised, including for Bring Your Own Device (BYOD). Supervision is managed through Apple Business Manager and further configured via an MDM, as outlined later in this guide. Supervision of devices handling classified data is necessary to ensure that the correct policies and configurations are applied throughout the lifecycle of the devices. Organisations will need to register with Apple to create Business Manager Accounts and Apple IDs. For high-risk implementations of devices, and cases where registering with Apple is neither desirable nor technically feasible, advice may be sought from ASD on potential alternatives.

The need for supervision of BYOD is a serious consideration for individuals wishing to work using their own devices, as it effectively hands control of devices over to an organisation. Therefore, a detailed discussion about the need for BYOD should be held between the user and authorising officer, with appropriate policy developed to support this requirement.

Advice to authorising officers

ASD has developed the *Strategies to Mitigate Cyber Security Incidents* to help organisations and their authorising officers mitigate risks caused by various cyber threats. The most effective of these mitigation strategies are known as the Essential Eight. While the strategies were developed for Microsoft Windows workstations and servers, much of this is applicable to modern smartphones.

iOS 14 and the Essential Eight

Application control

- When configured in accordance with ASD guidance, iOS 14 implements application control that is enforced via cryptographic signatures. iOS platform application control provides sufficient granularity to allow an administrator to approve specific versions of applications.

Patch applications

- Patches for applications are made available to devices as soon as they are released. When configured in accordance with ASD guidance, system administrators are able to remotely apply patches to organisation-owned and supervised devices.

Configure Microsoft Office macros settings

- The iOS platform does not support high-risk features such as Microsoft Office macros.
- However, new versions of Microsoft Office for iOS may introduce macro functionality and will not be separated from bundled security enhancement patches. Authorising officers will need to be aware that further configuration and reassessment of their exposure to this risk may be required in the future.

User application hardening

- When configured in accordance with ASD guidance, at risk applications such as web browsers are secured by not supporting Java and by using content blocker solutions.

Restrict administration privileges

- The iOS platform restricts administrator permissions by default for both the user and applications.

Patch operating systems

- iOS platform operating system patches are made available directly to devices as soon as they are released. When configured in accordance with ASD guidance, system administrators are able to remotely apply patches to organisation-owned and supervised devices.

Multi-factor authentication

- When configured in accordance with ASD guidance, devices and user identities are authenticated through multiple authentication factors.

Daily backups

- The iOS platform supports remote backups of some content to solutions approved by organisations. Further decisions can be made beyond ASD guidance to further improve the maturity level of daily backup solutions.

iOS 14 platform feature summary and risk considerations

Supervised Mode (Applicability: Organisation-owned device)

OFFICIAL: Sensitive	PROTECTED
Required	Required

Risks

Without this mode, devices may not always comply with an organisation's controls and misplaced devices cannot be secured remotely.

All organisation-owned devices are required to be supervised. Supervision of devices enables an organisation to enforce broader device policy, monitor the status of devices, manage Activation Lock and enable Lost Mode. Devices that handle classified data, or interact with an organisation's systems, are required to use Supervised Mode via Apple Business Manager and an MDM.

The use of Supervised Mode prevents users from being able to sync or backup device contents to home computers and ensures that users cannot easily sidestep restrictions without erasing all data from devices. Additionally, iOS forensic recovery utilities will not be able to recover data from devices without the use of a jailbreak.

Supervised Mode increases the difficulty of a number of attacks that rely upon the USB host-pairing protocol. Supervised Mode also allows an MDM to manage Activation Lock.

Additional information can be found under the 'Organisation-owned mobile devices' topic in the ISM.

Supervised Mode (Applicability: Bring Your Own Device)

OFFICIAL: Sensitive	PROTECTED
Required	Required

Risks

Without this mode, devices may not always comply with an organisation's controls and misplaced devices cannot be secured remotely. Organisations will also have a reduced ability to enforce security, audit and monitoring of non-supervised BYOD.

An organisation's BYOD deployment model will impact upon the residual risk of the deployment. As such, organisations should decide whether BYODs are to be supervised. Supervision of devices enables an organisation to enforce broader device policy, monitor the status of devices, manage Activation Lock and enable Lost Mode. BYODs that handle classified data, or interact with the organisation's systems, should use Supervised Mode via Apple Business Manager and an MDM.

Additional information can be found under the 'Privately-owned mobile devices' topic in the ISM.

Device passcode

OFFICIAL: Sensitive	PROTECTED
Required	Required

Risks

ASD provides guidance on creating strong passwords/passphrases. Should this not be followed, the encryption strength afforded to data at rest will be significantly diminished where devices are lost or stolen.

A sufficiently long and complex device passphrase ensures that devices are appropriately protected while locked, by ensuring that passcodes are both difficult to guess and that enough entropy is generated by the user credentials to derive adequate ephemeral keys.

Additional information can be found under the 'Single-factor authentication' topic in the ISM.

Biometric device unlock

OFFICIAL: Sensitive	PROTECTED
Organisation decision	Not allowed

Risks

When supported by a sufficiently strong device passcode, there is no difference in risk between using TouchID and FaceID. Deployments of iOS devices using biometrics should consider the practicality and privacy of users, and tailor advice surrounding these features to best suit the deployment scenario. Authorising officers should seek ASD guidance to assess these considerations where a tangible practical demand for biometrics is identified.

The biometric mechanisms of the iOS platform have not undergone an ACE, and the security claims of the feature are difficult to assess. The use of TouchID and FaceID to protect classified data may be considered for **OFFICIAL: Sensitive** deployments, however, must not be used when the device handles **PROTECTED** data.

Additional information can be found under the 'Authentication hardening' section in the ISM.

Non-native applications

OFFICIAL: Sensitive	PROTECTED
Organisation decision	Organisation decision

Risks

Applications that do not handle classified data appropriately, or afford a suitable level of encryption, are at risk of disclosing or mishandling of classified data.

Non-native applications are sourced from the App Store (either the public App Store or Custom Apps) or from an internal organisational source that uses Apple Developer Enterprise Program (including applications developed internally by an organisation for specific use on the iOS platform).

Organisations considering the deployment of non-native applications should carefully review the data at rest and data in transit mechanisms offered by the developer to ensure that appropriate encryption mechanisms are implemented. Data at rest solutions must make use of 'Class A' data protection for **PROTECTED** deployments.

Additional information can be found under the 'Application hardening' section in the ISM.

Mobile Device Management

OFFICIAL: Sensitive	PROTECTED
Organisation decision	Required

Risks

Without an MDM solution, devices may not always comply with an organisation's controls and misplaced devices cannot be secured remotely.

The iOS platform allows organisations to automatically manage device enrolment through the Apple Business Manager platform. MDM solutions allow for configuration management, deeper inspection and auditing of devices, as well as device content such as applications and documents. In certain limited circumstances, it may also be appropriate to use Apple Configurator as an alternative to, or in conjunction with, a dedicated MDM solution. Using an MDM solution allows an organisation to vet and deploy applications without user action or by using iTunes.

Through MDM solutions, notifications can be muted for managed applications and only allowed to be active under given circumstances (e.g. only allow notifications when an application is active). It is recommended that notifications only appear for managed applications when devices are unlocked. This recommendation is applied at the **OFFICIAL: Sensitive** and **PROTECTED** levels. It is recommended that managed applications be configured through a MDM solution to not be removable, to avoid users inadvertently uninstalling allowed applications.

Organisations implementing MDM solutions are encouraged to select products evaluated against the *MDM Agent* module of NIAP's MDFPP.

Organisations operating in higher risk situations are encouraged to engage with ASD when developing and implementing MDM solutions.

Additional information can be found under the 'Mobile Device Management' topic in the ISM.

Bring Your Own Device

OFFICIAL: Sensitive	PROTECTED
Organisation decision	Not recommended

Risks

BYODs have a higher risk of inadvertently introducing malware into an organisation's networks, and are at higher risk of infection with malicious applications or software before they are configured for handling classified data. Therefore, organisations should understand the risks around allowing privately-owned devices onto their networks, and ensure they follow ASD guidance.

As long as a device is enrolled in an MDM and is appropriately configured, devices handling **OFFICIAL: Sensitive** data can be BYOD.

Additional information can be found under the 'Privately-owned mobile devices' topic in the ISM and the *Risk Management of Enterprise Mobility (Including Bring Your Own Device)* publication.

Managed Open-In

OFFICIAL: Sensitive	PROTECTED
Required	Required

Risks

Devices not correctly configured for Managed Open-In, risk allowing un-assessed applications from being loaded onto devices. These applications may not meet data at rest and data in transit requirements for handling classified data.

Managed Open-In is built into the iOS platform and configured by MDM solutions. Managed Open-In allows organisations to decide which applications or accounts configured on devices can access classified data. Even if devices are configured in a 'work only' mode with no personal enablement, Managed Open-In can be used to ensure **PROTECTED** data is only held in, and moved between, applications that have appropriate data at rest and data in transit protections implemented.

In-app accounts will need to be managed properly as users can manually switch from an enterprise account to a personal account of a managed Open-In application.

Additional information can be found under the 'Application control' and 'Hardening application configurations' topics in the ISM.

Virtual Private Network

OFFICIAL: Sensitive	PROTECTED
Required	Required

Risks

Not using a VPN risks exposing data (and metadata) in transit to increased visibility by any entities on the networks the data traverses. This may increase an organisation's attack surface, as alternatives may require servers to be directly connected to the internet.

All data communicated by devices handling classified data must be through a VPN. Typically, BYOD and Corporately Owned, Personally Enabled (COPE) configurations will use a 'per-app' VPN, but some deployments will have a risk profile where they are required to use a whole device 'always on' VPN configuration. The built-in IPsec IKEv2 VPN client can be configured via profile for either type. This can be changed dynamically to suit the deployment requirements.

'Per-account' VPN allows managed accounts to be channelled through a specific VPN tunnel. This allows multiple email accounts to be pushed by MDM through separate VPN tunnels, yet still be inside the Managed Open-In boundary. For example, Microsoft Exchange has two emails accounts (one for **OFFICIAL** and another for **PROTECTED**) each one connected through a separate VPN tunnel on the same device.

'Per-app, per protocol' VPN allows exceptions from either per-app VPN or always on VPN, through MDM policy. The primary use-case is for Voice over Internet Protocol (VOIP) / Unified communications (UC) applications that use User Datagram Protocol (UDP), but could apply to downloading public data such as mapping data outside of a VPN tunnel. Misconfigurations of the per-app, per protocol VPN can potentially introduce a vulnerability into deployments.

Addition information can be found under the 'Connecting mobile devices to the internet' topic in the ISM.

Backups

OFFICIAL: Sensitive	PROTECTED
Organisation decision	Organisation decision

Risks

Without regular backups, classified data may be irrecoverable should only a local copy of the data exist and become inaccessible. However, with unapproved backup solutions, classified data may be extracted and then stored on, or transit over, systems that are not suitable for the sensitivity or classification of the data.

The configuration of devices is set by an MDM solution, and is restored whenever a device is enrolled. Whether backups are necessary depends on the nature of applications in use on devices. For example, email or chat applications are almost always synchronised with backend server storage, and thus do not require a backup from devices.

If data of organisational value is being created on devices, careful application selection or development can negate the need for organisational data to require backup explicitly from devices, because it is synchronised to servers implicitly (such as using a Content Management System that has a client with a File Sharing Extension). Note that in BYOD or COPE configurations, backup of personal content is generally desirable for users but covered by consumer solutions such as iCloud backup. Managed applications and accounts containing classified data can be excluded from the backups of personal content using appropriate configuration from a MDM solution.

Additional information can be found under the 'Data backup and restoration' section in the ISM.

Email applications

OFFICIAL: Sensitive	PROTECTED
Organisation decision	Organisation decision

Risks

Devices may over-classify all emails if they aren't able to be marked individually by the originator, as they may be set to the maximum sensitivity or classification by default. Alternatively, devices may under-classify all emails if there is no protective marking set by email clients or servers.

If an email client does not support the application of protective markings to emails, organisations should consider configuring email servers to allow for manual protective marking of emails by users. In some cases, installing a managed keyboard, to simplify marking of emails, will be more convenient for users than manually typing out protective markings.

The native email client on iOS is approved for **PROTECTED** data when configured in accordance with ASD guidance. See the *iOS Encryption* section for more details.

Additional information can be found under the 'Email usage' section in the ISM.

Microsoft Office for iOS

OFFICIAL: Sensitive	PROTECTED
Organisation decision	Organisation decision

Risks

iOS devices do not currently run Microsoft Office macros and therefore many of the risks associated with handling Office documents are not relevant at this time. As this is a feature of a third-party vendor, continual monitoring of this risk will need to be undertaken.

Organisations looking to implement Microsoft Office for iOS should refer to the 'Application hardening' section in the ISM.

iOS Calendar

OFFICIAL: Sensitive	PROTECTED
Organisation decision	Not Recommended

Risks

Should there be classified data in iOS Calendar data and metadata, these will not be stored with sufficient protection for classified data.

iOS Calendar allows synchronising calendar entries across accounts and devices. The iOS Calendar interacts with other applications to detect dates and times and suggest entries to be submitted to the calendar.

When using the iOS Calendar, attachments are afforded Class A data protection, but calendar data and metadata (such as the title of an event and any notes or details) are afforded only Class C protection. Therefore, authorising officers should make an informed risk decision about the use of the iOS Calendar for **OFFICIAL: Sensitive** data, and should not include **PROTECTED** data in any iOS Calendar event other than within calendar attachments.

iOS Contacts

OFFICIAL: Sensitive	PROTECTED
Organisation decision	Not recommended

Risks

iOS Contacts does not store details with sufficient protection for classified data.

iOS Contacts implements specific controls set by a MDM solution for the flow of contact information between managed and unmanaged spaces. For example, whether a managed contact can be used to display a person's name at the lock screen, instead of their phone number for an incoming call.

iOS Contacts data is stored on the device in a Class C container and, if names and phone numbers are considered **PROTECTED** data by an organisation, consideration should be given to using a dedicated application to manage such contacts.

iOS Camera

OFFICIAL: Sensitive	PROTECTED
Organisation decision	Not recommended

Risks

Photos and videos taken with iOS Camera are stored locally and may be transferred automatically to locations that do not have sufficient protection for classified data.

In BYOD and COPE devices, or deployments where photographs may be considered **PROTECTED** data, consider using a dedicated purpose-built camera app that stores photos in a Class A container.

iOS Camera uses Class C data protection to store photographs, and depending on the configuration set by a MDM solution, may be allowed to synchronise data to iCloud Photo Stream or to a user's personal unmanaged device.

iOS Books

OFFICIAL: Sensitive	PROTECTED
Organisation decision	Not recommended

Risks

iOS Books does not store data with sufficient protection for classified data.

A MDM solution can push iBook, ePub and PDF documents into iOS Books on devices. Such documents are considered managed by built-in controls and are not included in backups, nor can they be moved to unmanaged destinations or synchronised to iCloud. However, any **PROTECTED** documents must use a dedicated application that uses Class A data protection.

iOS Books uses Class C data protection, so it is only suitable for **OFFICIAL: Sensitive** or below documents.

Additional information can be found under the 'Application hardening' section in the ISM.

Location services

OFFICIAL: Sensitive	PROTECTED
Organisation decision	Organisation decision

Risks

Through the use of location services, information based on devices' physical location is obtained and used by Apple and third-party applications for various location-based services. To determine the location of devices, location services can use GPS, Bluetooth, crowd-sourced Wi-Fi hotspots and cellular tower locations.

Configuration by a MDM solution can control when location services are used (e.g. allow once, allow when active and always allow) and accuracy (precise or approximate).

Additional information can be found under the 'Radio Frequency devices' topic in the ISM.

Multi-factor authentication

OFFICIAL: Sensitive	PROTECTED
Recommended	Recommended

Risks

If multi-factor authentication is not implemented for application accounts on devices, compromised login credentials would allow unauthorised access to devices. Multi-factor authentication, when using biometrics, also provides an additional layer of security that strongly binds the identity of the user to a device. Note however, the authentication of the user to a MDM solution only occurs at device enrolment.

Additional information can be found under the 'Multi-factor authentication' topic in the ISM.

Domain Name System

OFFICIAL: Sensitive	PROTECTED
Recommended	Recommended

Risks

The protection of the Domain Name System (DNS) service is critical for the translation of Uniform Resource Locator (URL) addresses to Internet Protocol (IP) addresses. Starting from iOS 13, new features around the use of a DNS proxy to channel all DNS resolution via a secure channel, or using encrypted DNS, were introduced.

Additional information can be found under the 'Host-based intrusion prevention system' and 'Software firewall' topics in the ISM.

Additional considerations

iOS 14 introduces a number of new security features to the Apple iOS platform. For example, iOS 14 will attempt to randomise the MAC address when there is a network probe from a new network. Through MDM configuration, this feature can be disabled for instances when the iOS platform is connecting to an organisation owned and controlled network. In addition, as of iOS 14, Siri now processes user requests locally and single sign-on (SSO) extensions, used for authentication, will support per application VPN connections allowing a list of associated and excluded domains to interact with particular per application VPN configurations.

Glossary of cyber security terms

Term	Meaning
application control	An approach in which only an explicitly defined set of approved applications permitted to execute on systems.
ASD Cryptographic Evaluation	The rigorous investigation, analysis, verification and validation of cryptographic software and equipment by ASD against a stringent security standard.
authorising officer	An executive with the authority to formally accept the security risks associated with the operation of a system and to authorise it to operate.
classification	The categorisation of information or systems according to the business impact level associated with that information or system.
Common Criteria	An international standard for software and IT equipment evaluations.
cryptographic software	Software designed to perform cryptographic functions.
cyber security	Measures used to protect systems and information processed, stored or communicated on such systems from compromise of confidentiality, integrity and availability.
cyber security incident	An occurrence or activity that may threaten the confidentiality, integrity or availability of systems or information.
data at rest	Information that resides on media or a system.
data in transit	Information communicated across a communication medium.
integrity	The assurance that information has been created, amended or deleted only by authorised individuals.
Internet Protocol Security (IP Sec)	A suite of protocols for secure communications through authentication or encryption of Internet Protocol packets as well as including protocols for cryptographic key establishment.
IT equipment	Any device that can process, store or communicate electronic information.
key management	The use and management of cryptographic keys and associated hardware and software. It includes their generation, registration, distribution, installation, usage, protection, storage, access, recovery and destruction.

media	A generic term for hardware, often portable in nature, which stores information.
mobile device	A portable computing or communications device. For example, a laptop, mobile phone or tablet.
NFC	Near-Field-Communication, a set of communication protocols used between two electronic devices in close proximity.
passphrase	A sequence of words used for authentication.
password	A sequence of characters used for authentication.
patch	A piece of software designed to remedy vulnerabilities, or improve the usability or performance of software and IT equipment.
product	A generic term used to describe software or hardware.
protective marking	An administrative label assigned to information that not only shows the value of the information but also defines the level of protection afforded to it.
Protection Profile	A document that stipulates the security functionality that must be included in Common Criteria evaluation to meet a range of defined threats. Protection Profiles also define the activities to undertaken to assess the security function of an evaluated product.
security risk	Any event that could result in the compromise, loss of integrity or unavailability of information or resources, or deliberate harm to people measured in terms of its likelihood and consequences.
server	A computer that provides services to users or other systems. For example, a file server, email server or database server.
system	A related set of hardware and software used for the processing, storage or communication of information and the governance framework in which it operates.
system manager	An individual that the system owner has delegated the day-to-day management and operation of a system.
system owner	The executive responsible for a system.
user	An individual that is authorised to access a system.
Virtual Private Network	A private data network that maintains privacy through a tunnelling protocol and security procedures. VPNs may use encryption to protect traffic.
workstation	A stand-alone or networked single-user computer.

Further information

The *Information Security Manual* is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the *Strategies to Mitigate Cyber Security Incidents*, along with its Essential Eight, complements this framework.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).