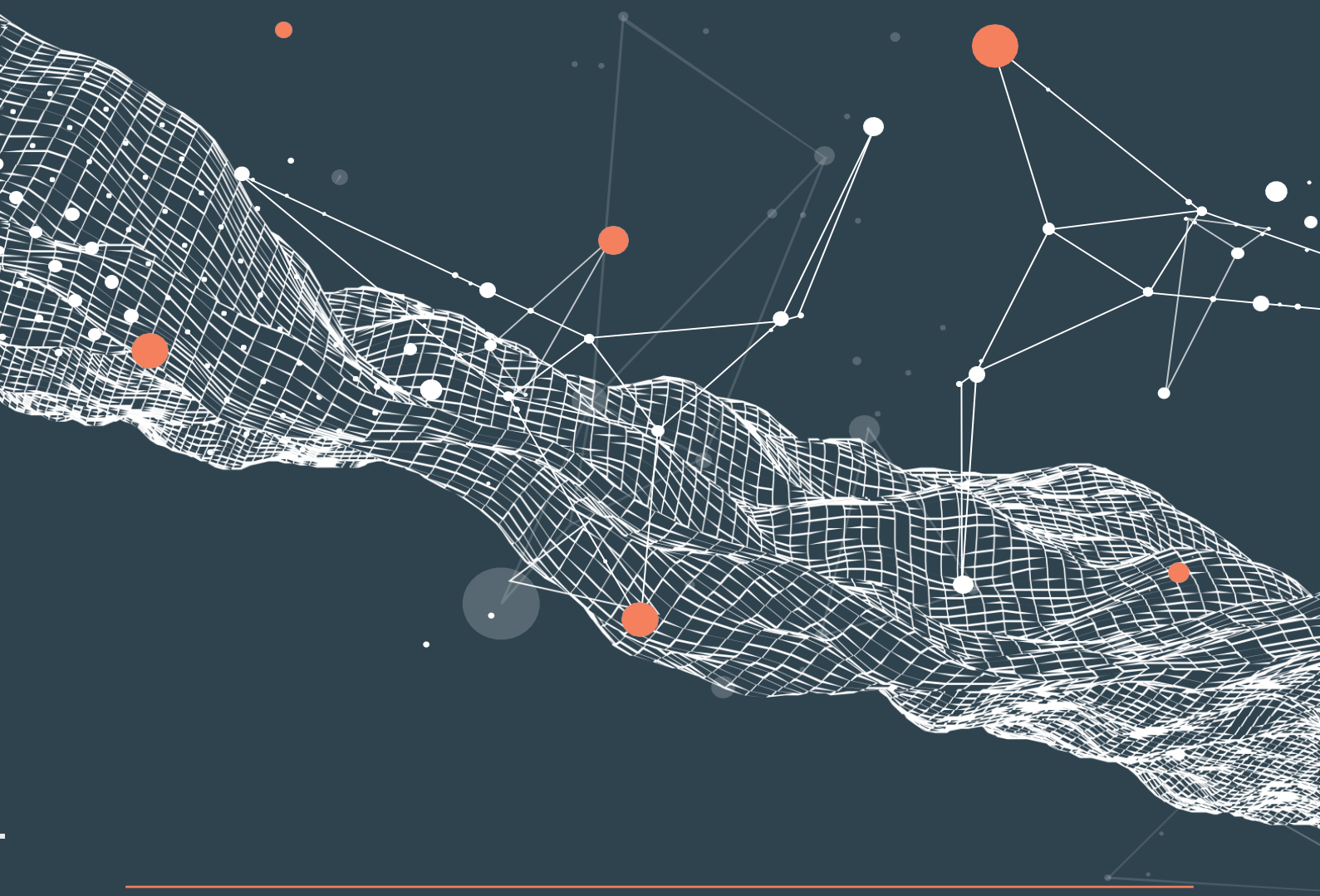
Australian Government

Department of Home Affairs



Australian Code of Practice for App Store Operators and App Developers

Discussion Paper

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

P-23-02503-c

Contents

Introduction

Under the Action Plan for Horizon 1 of the *2023-2030 Australian Cyber Security Strategy* the Government committed to co-design a voluntary cyber security Code of Practice for app stores and app developers. This initiative is a key step in the Government's efforts to embed cyber security into software development practices and to more clearly provide guidance on actions that app stores and developers can take to protect consumers and businesses from cyber attacks.

Apps, or applications, are a common feature in Australians' everyday life and are often used to access essential services, utilities, work, education and leisure activities. Apps are ubiquitous in our economy and are easily accessible through mobile phones, tablets and other smart devices. Many smart products and devices used by businesses and individuals require a companion app on the users' smart phone or tablet to be able to function.

While the use of apps enhances our everyday lives, apps can also present a cyber security risk to consumers. Many apps now collect sensitive and personal information, track location data, and can potentially act as a gateway for malware onto a user's network. Software and app developers are not currently required under Australian law to incorporate cyber security standards into their products. App users also face information asymmetries when downloading apps, often not being able to differentiate between the levels of cyber security of comparable apps or understand exactly how their data and personal information will be used, stored and shared.

Research has shown that the rapid growth in the consumer app and smart product market has outpaced the adoption of good cyber security practices (UNSW and ACCAN 2017). There is an increasing risk for Australian consumers, with recent media reports highlighting a specific case where over 180 malicious apps were removed from a popular app store with over 56 million downloads between them (Forbes 2025). A threat report from the UK's National Cyber Security Centre also identified several cases of malicious or unsecure apps being sold across mobile app stores, including on popular marketplaces like Apple's App Store, Google Play store, Steam, and Fitbit gallery (NCSC 2022).

Recognising that app stores are currently the most effective point of intervention to protect users at scale from malicious and insecure apps, as a first step, the Australian Government is seeking to work with industry and our international partners to develop a voluntary Code of Practice for our domestic context that will clearly communicate expectations of cyber security in software development.

Australia's app development industry is relatively small compared to the international landscape and many apps and app stores are not unique to the Australian market. Of the almost two million apps available on Google Play, roughly 8,000 were built by Australian developers – less than one per cent. Likewise, Australian consumers make up less than one per cent of global app downloads.

To ensure uptake of a Code of Practice in Australia and safeguard access to new apps for Australian users, it is essential that we seek to leverage existing international approaches where possible and appropriate. This will ensure that we don't add additional compliance obligations to Australian app stores and developers causing them to avoid the Australian market and restrict consumer choice, or risk applying standards that put Australian businesses at a competitive disadvantage.

With the growth of local technology start-ups and the continued digitisation of our economy, an opportunity arises for Australian app developers to support the vision of becoming a world leader in cyber security by building apps aligned with secure-by-design and secure-by-default best practices.

Background

Uplifting the security of app stores and consumer apps in Australia is challenging, due to Australia's relatively small footprint in the app store operator and developer markets and the government's limited jurisdiction to ensure app security when app store operators and developers are mostly domiciled overseas. A voluntary Code of Practice for App Store Operators and App Developers adopted by industry would provide a key market signal, and incentivise the necessary step-change needed to embed secure-by-design practices in consumer software applications. The Code of Practice will be voluntary so as to not impose regulatory burden on industry, but will set a cyber security 'benchmark' that industry can use when designing consumer apps, aligned with international best practice, so as to not disadvantage Australian businesses.

This introduction of a voluntary Code of Practice follows calls from industry for clear government guidance on what constitutes "basic cyber security" for apps. The Code of Practice needs to be calibrated for the Australian market, but importantly should align with international best practice, especially the UK's Code of Practice for App Store Operators and App Developers, which was introduced in December 2022.

The UK Government's Code could be a useful model to consider, with necessary adjustments if required to ensure that the Code is fit for purpose for Australian industry. If appropriate, the Australian Government could then consider options to adopt the Code, including the potential for co-sealing the UK Code of Practice in its entirety to ensure harmonisation of best practice principles across jurisdictions.

For the voluntary Code of Practice to be successful in Australia, it will need to set out practical steps for App Store Operators and App Developers to protect users. The UK model provides eight principles, in no order of priority, that refer to globally recognised security and privacy practices.

The responsibility to implement the principles falls on App Store Operators, App Developers and Platform Developers. However, given the role of App Store Operators in setting policies and processes for their app stores, reasonable steps should be taken by them to verify that App Developers and Platform Developers are adhering to the principles set out in the Code.

This discussion paper seeks to open the dialogue with industry to explore the idea of adopting an existing Code of Practice that is also appropriate to the Australian market, or developing one unique to the Australian context based on similar principles. The key principles outlined in the UK's Code of Practice are outlined below:

UK Code of Practice Key Principles

1	Ensure only apps that meet the code's security and privacy baseline requirements are allowed on the app store
2	Ensure apps adhere to baseline security and privacy requirements
3	Implement a vulnerability disclosure process
4	Keep apps updated to protect users
5	Provide important security and privacy information to users in an accessible way
6	Provide security and privacy guidance to Developers
7	Provide clear feedback to developers
8	Ensure appropriate steps are taken when a personal data breach arises

Through this discussion paper, the Australian Government is seeking feedback from industry to understand if the UK's Code of Practice would be appropriate for the Australian context, and if so how we can tailor the UK's Code of Practice to the Australian environment. The UK Code of Practice in full is outlined at the end of this paper.

Audience

The below stakeholders would be the main organisations adopting and implementing the Code of Practice in their operations:

Stakeholder	Description
App Store Operators	The persons or organisations responsible for operating the app store. The App Store Operator will have capability to add and remove apps. They will also decide on the requirements that apps will need to meet to be included in the app store, taking into account any legal requirements.
App Developers	Persons or organisations which create or maintain apps on the app store. App Developers are responsible for ensuring their app meets the requirements of the app store, as well as any legal requirements.
Platform Developers	Persons or organisations responsible for producing the operating system, default functionality and the interface that enables third parties to implement additional functionality, such as through apps.

Table 1 - Primary stakeholders for the Code of Practice

Aligning with the UK's Code of Practice, the Government proposes that Business-to-Business application programming interface (API) providers are not required to comply with the Code because it is the Developers' responsibility to understand what API codes/services they use and then develop their apps.

Key Terms

The below definitions are provided from the UK's Code of Practice for consideration for use in a potential Australian Code of Practice.

Term	Definition
App Store	A digital marketplace that allows users to download apps created by developers, including developers other than the app store's developers. App stores do not only host apps, as they also serve as storefronts that allow users to browse for apps, such as via search functionality.
Malicious app	A malicious app is one which intentionally seeks to illegally take user data, money, or control of their device, outside of the understood purpose of the app. It also incorporates apps that make a user or device undertake illegal activity. Indications that an app is malicious include (but are not limited to) phishing for credentials or illicitly collecting multiple types of sensitive data (e.g. contacts, messages), coupled with indicators of detection evasion such as obfuscation, dynamic loading, or cloaking of malicious behaviour.
Vulnerabilities	A vulnerability is a weakness in an app that may be exploited by an attacker to deliver an attack. They can occur through flaws and features, and attackers will look to exploit any of them, often combining one or more, to achieve their end goal.

Table 2 - Definitions for the potential Australian Code of Practice

UK Code of Practice

The following section provides detail on the UK's Code of Practice as a potential model for Australia to adopt.

The *UK Code of practice for app store operators and app developers* is based around eight principles. The UK Code of Practice followed a public consultation period which received 59 responses. The vast majority of respondents supported all principles within the voluntary Code of Practice and the need for the code.

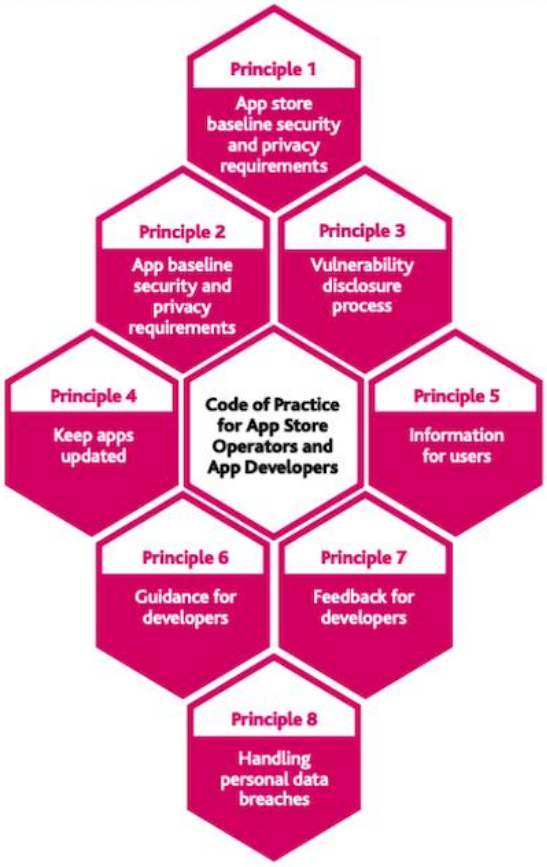


Figure 1 - Principles for the Code of Practice for App Store Operators and App Developers

Ensure only apps that meet the code's security and privacy baseline requirements are allowed on the app store

Primarily applies to: **App Store Operators**

1.1 App Store Operators shall clearly set out security and privacy requirements for apps on the app store, published in a location that does not require purchasing access by Developers. This shall include those provisions set out in principle 2.

1.2 App Store Operators shall have a vetting process which includes security checks in which the above security and privacy requirements are reviewed prior to approving app submissions and updates. Operators shall notify the Developer if an app or update is rejected for security reasons (see principle 7 for more detail).

1.3 App Store Operators shall provide a high level overview of the security checks that are undertaken for apps and updates in a publicly accessible location.

Example of information provided by an Operator on their security checks

Apps undergo a security check which consists of both automated and manual activities. These checks include confirmation with developers on the necessity of the permissions they are requesting, confirmation of Software Development Kit versions, scanning for default credentials, and the use of analysis tools.

1.4 App stores shall have an app reporting system (such as visible contact details or a contact form), so that users and security researchers can report malicious apps, and Developers can report fraudulent copies of their own apps to the app store.

1.5 Once an App Store Operator has verified that an app is clearly malicious, they shall make the app unavailable on the app store as soon as possible but no later than 48 hours. Operators shall notify the Developer that their app has been removed or made unavailable. Operators shall have an appeals process in place which gives Developers 7 days from receipt of the notification to challenge the removal decision.

1.6 Once an App Store Operator verifies that an app or an update is malicious, they should initiate a proportionate review of other apps that have been produced by the same developer account.

1.7 App Store Operators and Developers should consider working with independent parties to assess app security and privacy.

Ensure apps adhere to baseline security and privacy requirements

Primarily applies to: **App Developers** and **Platform Developers**

2.1 Developers shall use industry standard encryption within their apps, specifically in relation to data in transit and where an app needs to encrypt data locally.

Apps utilise, receive and transmit data that is often sensitive in nature. This may include data relating to users, an enterprise, functionality or other information necessary for the app to operate securely. This data needs to be encrypted at rest and in transit in order to ensure it cannot be compromised by an attacker.

This may be done by APIs native to the platform, which will often integrate with secure hardware on the device.

2.2 Developers shall ensure that the primary function of an app operates if a user chooses to disable its optional functionality and permissions.

2.2.1 If the user is not presented with any optional functionalities, developers shall ensure that their app only requires the enabled functions and permissions necessary to operate.

2.3 Developers should not request permissions and privileges which are not functionally required by the app.

2.3.1 Developers shall share the permissions and privileges requested by the app in the app manifest with the App Store Operator, to allow for this to be cross-checked.

A functional requirement is defined as one that is necessary for the user-facing operation of the app. This does not include any background operation which does not offer the user any features or an improved experience.

2.4 Developers shall take steps to make their app adhere to security requirements, data protection by design, broader requirements set out in data protection law and other appropriate laws to the app's purpose.

2.5 Developers shall ensure there exists a simple uninstall process for their app.

2.6 Developers should have a process to readily update and monitor their software dependencies for known vulnerabilities in all the published versions of their app.

2.7 Developers shall provide users with a mechanism to and request deletion of personal data gathered by an app.

Implement a vulnerability disclosure process

Primarily applies to: **App Developers** and **App Store Operators**

3.1 Every app shall have a vulnerability disclosure process, such as through contact details or a contact form, which is created and maintained by the Developer, and accessible within the app store.

3.2 Operators shall check that every app on their platform has a vulnerability disclosure process which is accessible and displayed on their app store. This process shall ensure that vulnerabilities can be reported without making them publicly known to malicious actors.

3.3 App Store Operators shall ensure their app store has a vulnerability disclosure process, such as contact details or a contact form, which allows stakeholders to report to the Operator any vulnerabilities found in the app store platform.

3.3.1 App Store Operators should accept vulnerability disclosure reports from stakeholders for apps on their platforms if the Developer has not issued an acknowledgement to said report. App Store Operators should assess the merit of these reports, and contact the Developer if they are deemed credible.

3.3.2 If App Store Operators do not receive an acknowledgement from the Developer, they should make the app unavailable on the store.

Keep apps updated to protect users

Primarily applies to: **App Store Operators**, **App Developers** and **Platform Developers**

4.1 Developers shall provide updates to fix security vulnerabilities within their app.

4.2 Developers shall update their app when a third-party library or software development kit (SDK) that they are using receives a security or privacy update. See principle 6.4 for the proposed actions on App Store Operators.

4.3 When a Developer submits a security update for an app, App Store Operators shall encourage users to update the app to the latest version.

4.4 App Store Operators shall not reject standalone security updates without providing a strong and clear justification to the Developer as to why this has happened. In cases where an Operator is not approving the update due to concerns that they are engaging with a malicious Developer, an Operator shall have flexibility on the time period and detail of said feedback.

> A standalone security update is one which affects only the security and privacy functionality of the app, with no changes to user functionality, or non-security background operation.

4.5 App Store Operators shall contact a Developer if an app has not received an update for 2 years to check that the app is still being supported.

4.5.1 If the Operator does not receive a response from this process within 30 days, then they should consider making the app unavailable on the store.

Provide important security and privacy information to users in an accessible way

Primarily applies to: **App Store Operators** and **App Developers**

5.1 When an app is removed or made unavailable from an app store, the Operator shall provide this information to users of said app (for example, through push notifications or a page in the app store)

and link to instructions on how a user would remove the app from their device within 30 days. If a developer has challenged a removal decision on an app that has not been deemed malicious, users shall not be notified until the appeals process has concluded.

5.1.1 The App Store should have functionality to present to users which apps they have downloaded and installed that are no longer available on the app store.

> The term “unavailable” refers to when an app is hidden from new users so they cannot download the app, but may still be on the app store so current users may be able to receive updates.
>
> The term “removed” includes when an app is completely removed from the app store; this could be by either the operator or developer. This may be for security or other reasons.

5.2 Developers shall provide the following information about an app’s behaviour: where a user’s data is stored, shared and processed within a privacy policy; when the app was last updated; and other relevant security and privacy information.

5.3 App Store Operators shall display the below information (provided by Developers) for all apps on their app store, such as in a dedicated security and privacy section for users:

5.3.1 The jurisdictions where a user’s data is stored and processed for each app.

5.3.2 The stakeholders that are given access to a user’s data. The categories of stakeholders that are displayed to a user should include third party companies, the app’s organisation, specific governments or not shared with anyone.

5.3.3 The purpose of accessing or using a user’s data. Categories should include marketing, analytics, user services.

5.3.4 When the app was last updated and any other relevant security information, as well as the information linked to permissions noted in principle 2.

5.3.5 The above information shall be written in an accessible format for all users and be clearly available prior to purchase and download.

5.4 Developers shall provide information about the permissions which an app may request, such as access to contacts, location and the device’s microphone, along with justifications for why each of these permissions are needed. This information shall be provided to app stores and any users who install the app without an app store. Operators shall display this information for all apps on their app store prior to purchase and download.

Provide security and privacy guidance to Developers

Primarily applies to: **App Store Operators**

6.1 App Store Operators shall signpost this Code of Practice to Developers prior to an app’s submission.

6.2 App Store Operators should publicise any upcoming changes to be introduced to their Developer guidelines / policies.

6.3. App Store Operators should provide information on what is considered best security and privacy practice where that goes beyond the Code’s baseline requirements, such as information on other standards that have been produced.

6.4. App Store Operators should support App Developers in implementing effective supply chain management, such as by monitoring common third-party libraries and services and sharing relevant information, highlighting potential threat vectors across multiple apps.

Provide clear feedback to developers

Primarily applies to: **App Store Operators**

7.1. When an app submission is rejected, the App Store Operator should provide consistent and

actionable feedback, justifying the rejection of the app and making clear what elements would need to change in order for the app to be accepted.

7.2. When an App Store Operator removes or makes an app unavailable for security or privacy reasons, they shall notify the Developer of this step, and provide feedback explaining the reasoning behind the decision. Operators shall take into consideration that the feedback they provide does not help malicious actors.

Ensure appropriate steps are taken when a personal data breach arises

Primarily applies to: **App Developers** and **App Store Operators**

8.1. If an App Store Operator becomes aware of a security incident in an app which involves a personal data breach, they shall inform the app developer.

8.2. Developers should inform other relevant stakeholders such as App Developers, App Store Operators, and library/SDK Developers.

8.3. When Operators are notified about a personal data breach in an app, Operators should consider whether the app should be made unavailable to users.

Discussion Questions

1. **Do you think a voluntary Code of Practice will sufficiently uplift security processes in the Australian context for app store operators and developers, and provide clear guidance on actions that can be taken to protect consumers and businesses from cyber attacks?**
    - If no, what other approaches would you consider to be more effective?
2. **Is the UK Government's Code of Practice for app store operators and app developers a useful model to consider adopting for enhancing cyber security for apps in the Australian market?**
    - What else would you like to see included in the Code of Practice that isn't in the UK Government's Code to make applications more secure?
    - How important is it to have exact alignment to the UK Code?
3. **Are there challenges for Australian industry in adopting a Code of Practice like the UK Government's?**
    - If so, how can the Australian Government provide support?
    - What additional guidance would industry need in the Australian context to meet a Code of Practice?
4. **How would we best monitor the effectiveness of a Code of Practice to ensure that it is taken up and delivering positive outcomes for the app industry and consumers?**
5. **What other initiatives should the Australian Government pursue to secure apps for Australian consumers?**
    - What are the opportunities for government and industry collaboration in this space?

References

Forbes (2025) 'Google confirms Play Store app deletion—check your phone now', Forbes, accessed 25 March 2025.

NCSC (National Cyber Security Centre) (2022) *Threat report on application stores*, NCSC, accessed 25 March 2025.

UNSW (The University of New South Wales) and ACCAN (The Australian Communications Consumer Action Network) (2017), *Inside job: Security and privacy threats for smart-home IoT devices*, ACCAN, accessed 25 March 2025.

/