Australian Government

Department of Home Affairs

Australian Voluntary Code of Practice for App Store Operators and App Developers

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

Background

This voluntary Code of Practice sets out practical steps for App Store Operators and App Developers to protect users. The eight principles within the Code refer to globally recognised security and privacy practices. They are not written in a priority order as they are each important in helping to protect users' security and privacy.

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.

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

Figure 1 Code of Practice Key principles

Audience

An indication is given for each principle within this Code as to which stakeholder is primarily responsible for implementation. Stakeholders are defined as:

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.

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. This Code uses the Australian Taxation Office definition of APIs, which is as follows: "An API is a set of subroutine definitions, protocols, and tools for building application software. It is a software intermediary that allows two applications to talk to each other".

Key Terms

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.

1. 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.

2. 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 privacy and data protection laws 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

/