
BLACKTECHSTARTUP EDUCATION

Ship a Mobile App Without Getting Trapped by App Store Rules

Prepare an iOS and Android app for real distribution: privacy inventory, account deletion, store metadata, permissions, security, beta testing, review responses and post-launch operations.

Prepare an iOS and Android app for real distribution: privacy inventory, account deletion, store metadata, permissions, security, beta testing, review responses and post-launch operations.

Design for distribution before the app is finished

A mobile app is not just code. Distribution adds developer identities, signing keys, store records, privacy disclosures, screenshots, age/content answers, platform policies and review. Create the App Store Connect and Play Console release checklist while the product is still being built. If you wait until “the app is done,” policy requirements can force expensive redesigns.

Decide early whether you truly need a native mobile app. If the product can deliver its value through a responsive web app or PWA without deep device integration, starting on the web can reduce release friction. Choose native or cross-platform mobile when push, offline behavior, sensors, camera, Bluetooth, platform payments, background capabilities or app-store discovery materially improve the product.

Build a data map before answering privacy forms

List every data element the app and every embedded SDK collects: account identifiers, contact data, device identifiers, analytics, diagnostics, location, photos, files, purchases and anything sent to an AI or other third party. Record why it is collected, where it goes, retention, deletion path and whether it is

linked to identity. Apple requires developers to describe app and third-party-partner data practices in App Store privacy details; Google requires accurate Data safety disclosures. Do not fill these forms from memory.

Minimize collection. If you do not need precise location, do not request it. If an SDK collects more data than its business value justifies, replace it. Privacy labels are not a substitute for privacy engineering; they are a disclosure of what your engineering actually does.

Account creation creates an account-deletion obligation

Google Play states that if an app enables account creation, developers must provide an in-app path for users to delete the account and associated data and a web resource where deletion can be requested. Apple also has account-deletion requirements for apps that support account creation. Build deletion as a real server-side capability, not a fake “deactivate” screen. Decide what must be retained for lawful accounting, fraud or security reasons and explain that appropriately in your policy.

Test deletion from end to end: user initiates it, identity is verified, sessions are revoked, scheduled jobs stop, data is deleted or legitimately retained according to policy, third-party processors receive the appropriate request, and the user gets confirmation. The store reviewer should not be your first end-to-end deletion test.

Permissions need a product reason, not merely a technical reason

Ask for camera, microphone, contacts, photos, Bluetooth, location or notifications only when the user reaches the feature that needs them. The permission explanation should describe the user benefit in plain language. Test the app when every permission is denied; denial should not crash unrelated workflows. Provide a route to settings when the permission is essential later.

For AI-enabled apps, explicitly map whether user content leaves the device, which provider processes it and whether sensitive material can be sent. Privacy expectations can change as platforms update their review policies, so check current guidelines immediately before submission.

Use a mobile security standard and threat model

OWASP MASVS is a practical standard for mobile application security. Review storage, cryptography, authentication, network communication, platform interaction, code quality and resilience. Do not store tokens or sensitive secrets in ordinary local preferences. Use platform-secure storage where appropriate, TLS for network traffic, server-side authorization, short-lived sessions where feasible and explicit logout/session revocation.

Threat-model the device as something an attacker may control. Client checks can be bypassed. Premium access, account roles and critical business rules should be enforced by the server. Test rooted/jailbroken or instrumented conditions if your risk level warrants it, but do not mistake anti-tamper measures for core authorization.

Run three beta rings before public release

Ring 1 is the team: every core flow, supported OS version and device class. Ring 2 is trusted external testers who were not involved in building the app. Ring 3 is a limited real audience. Track crash-free sessions, login success, time to first value, permission denial behavior, network-loss behavior, payment/subscription state and support contacts. Give testers tasks rather than asking “Does it look good?”

Before store submission, perform a clean-install test on devices that have never had your app, then an upgrade test from the previous version. Many release failures hide in migration and first-run state.

Treat review as a reproducible test, not an argument

Provide review notes with test credentials, exact navigation to gated features, hardware requirements and explanations for unusual behavior. If rejected, map the rejection to the cited guideline, reproduce the reviewer’s path and fix the underlying issue. If you believe the review is wrong, respond with concise evidence and exact behavior. Angry review notes do not improve the product.

After approval, release gradually when the platform and your risk tolerance allow it. Watch crashes, reviews, support and server load. Be prepared to halt rollout or ship a corrective version. Mobile release is an operating capability, not a ceremony you perform once.

Research behind this guide

Use the primary and authoritative sources below to verify current rules, prices, eligibility and program details before acting. Terms can change.

Apple — App Review Guidelines



Apple — App Privacy Details



Apple — Offering Account Deletion



Google Play — Account deletion requirements



Google Play — User Data policy



OWASP — Mobile Application Security Verification Standard



Important: This guide is educational information, not individualized legal, tax, investment, employment, security or compliance advice. For decisions with material legal or financial consequences, use a qualified professional who can review your facts.

SHARE THIS GUIDE ↗

POWERED BY: BLACK TECH STARTUP

blacktechstartup.com