

Mobile Applications Development and Management Guidelines

As government institutions increasingly embrace mobile technology to deliver services and information to citizens, it becomes paramount to ensure that these applications adhere to standard guidelines to ensure that mobile applications meet user requirements, are easy to use, and meet security and data privacy requirements. By upholding these guiding principles, governments can harness the full potential of mobile technology to deliver seamless, secure, and citizen-centric services, thereby fostering public trust, participation, and empowerment.

- Introduction
- Scope and Objectives
- Considerations for mobile applications in Government
 - Approval Process [Mandatory]
 - Complementary delivery channels[Recommended]
 - Cost effective approach[Recommended]
- Design Guidelines

- Adopt platform design guidelines[Mandatory]
- Multi Language support[Mandatory]
- Responsive design[Mandatory]
- Accessibility[Recommended]
- Platform conventions[Recommended]
- Availability across platforms[Recommended]
- Official app stores[Mandatory]
- Device testing[Mandatory]
- Performance optimisation[Mandatory]
- Offline access[Recommendation]
- User involvement[Mandatory]
- Open standards[Mandatory]
- Branding[Mandatory]
- Monitoring analytics[Recommended]
- Security and data privacy
 - Security
 - Data privacy
- Maintenance of mobile applications
 - Monitoring analytics [Mandatory]
 - User support and feedback[Mandatory]
 - Compatibility to new device versions and software[Mandatory]
 - Regular updates[Mandatory]
 - Security maintenance[Mandatory]
 - Performance monitoring[Mandatory]

Introduction

In today's digital age, mobile applications have become indispensable tools for governments worldwide, fostering efficient communication, enhancing public services and facilitating citizen engagement. As government institutions increasingly embrace mobile technology to deliver services and information to citizens, it becomes paramount to ensure that these applications adhere to standard guidelines to ensure that mobile applications meet user requirements, are easy to use, and meet security and data privacy requirements. By upholding these guiding principles, governments can harness the full potential of mobile technology to deliver seamless, secure, and citizen-centric services, thereby fostering public trust, participation, and empowerment.

Scope and Objectives

This document outlines the guidelines for the development and management of mobile applications for Government of Rwanda institutions with the objective of making them citizen-centric and secure. They apply to all Government institutions which may wish to develop and deploy mobile applications to deliver citizens services or for internal automation of Government processes. Key objectives of these guidelines include:

- Ensure mobile application projects are initiated and implemented in line with existing policies to ensure alignment with wider technology strategies and current best practices
- Ensure applications meet the user requirements of the institution which is fundamental to the success and relevance of government mobile applications.
- Ensure that user centricity is a core part of the design and achieve applications that are easy to use for users. This will foster engagement and trust among citizens, empowering them to interact seamlessly with government services and information.
- Enable accessibility of the applications by diverse demographics, including those with disabilities or limited technological literacy.
- To ensure the applications meet security requirements particularly for government institutions handling sensitive data and transactions. Robust security measures, including encryption protocols, authentication mechanisms, and regular security audits, are imperative to safeguard against cyber threats and data breaches.
- To ensure compliance with data privacy requirements and regulations to protect personal data of users of government mobile applications , encompassing principles of consent, transparency, and accountability.

Considerations for mobile applications in Government

Increased access to the internet through mobile devices in Rwanda provides an opportunity to use mobile applications to deliver Government services in a convenient manner to more citizens. Mobile applications can also be used to improve efficiency of internal government processes. The following should be considered when adopting mobile applications in Government:

Approval Process [Mandatory]

- Mobile application projects should be approved before commencing and should follow the approval process defined in the RISA software lifecycle management guidelines and ICT spend control guidelines
- Once a mobile application is developed, written approval for publication should be obtained from RISA with information provided on the application's compliance to Government design and security guidelines

Considerations for mobile applications in Government

Complementary delivery channels[Recommended]

Mobile applications should not replace other Government service delivery channels but rather should complement them. Mobile applications should not be the only means of providing information or service

Mobile applications content should align with content that is available through other channels

Cost effective approach[Recommended]

Mobile applications should only be developed if they provide the best way option to deliver a service or automate a process. Developers should consider other alternatives such as creating a mobile optimised website which may be more cost effective and easier to adapt to changing technology and future needs

Design Guidelines

When designing mobile apps for various platforms and devices in Rwanda, it is important to consider the following to ensure a good user experience:

Design Guidelines

Adopt platform design guidelines[Mandatory]

Adhere to design guidelines and principles provided by each platform such as the Material Design for Android and Human Interface Guidelines for iOS

Multi Language support[Mandatory]

Consider support for local languages particularly Kinyarwanda when designing citizen facing mobile applications to increase accessibility.

Responsive design[Mandatory]

Adopt a responsive design approach to allow your application to adapt to different screen orientations. Use fluid layouts and scalable UI components that can adjust seamlessly to landscape and portrait modes.

Accessibility[Recommended]

Aim to ensure your app is accessible to users with disabilities. Implement features such as adjustable font sizes, support for screen readers, color contrast options, and alternative text for images. Follow RISA software accessibility guidelines to make mobile applications inclusive for all users.

Platform conventions[Recommended]

Consider the navigation patterns and gestures familiar to users on each platform. For example, use bottom navigation bars for Android and tab bars for iOS. Follow platform-specific conventions for swipe gestures, back buttons, and other navigational elements

Availability across platforms[Recommended]

To ensure availability across different platforms, mobile applications should at the very least be available on both Google's Android and Apple's iOS platforms, with priority for Android, which is the majority in Rwanda.

Official app stores[Mandatory]

To ensure safe and secure distribution of apps, official app stores should be used for public app distribution. Enterprise mobile apps, developed or purchased for internal use of the Government institution and not provision of public facing services should not be distributed publicly using an app store.

Device testing[Mandatory]

Test mobile applications on real devices representing the popular platforms and models used in Rwanda. This helps identify and address any device-specific issues, such as layout inconsistencies, performance bottlenecks, or compatibility problems.

Performance optimisation[Mandatory]

Optimise an app's performance by minimizing loading times, optimizing image sizes, and implementing efficient caching strategies. Test the app's performance on devices with varying capabilities and network conditions.

Offline access[Recommendation]

The mobile app should be developed in a way to cater for offline activity and reduce wherever possible frustration for the customer being outside a mobile coverage area. For example, if a customer completes a form within the mobile app without network connectivity they should be able to submit the form as soon as they return to network coverage.

User involvement[Mandatory]

Gather feedback from users in Rwanda during the design and testing phases. Incorporate user insights to improve usability, address pain points, and align the app's design with local preferences.

Open standards[Mandatory]

Open standards shall be adopted for mobile applications for ensuring the interoperability of applications across various operating systems and devices.

Branding[Mandatory]

Adhere to Government of Rwanda branding guidelines when designing mobile applications

Monitoring analytics[Recommended]

Apply appropriate analytics for monitoring the mobile app to gauge engagement and customer behaviour and to identify opportunities to improve the app

Security and data privacy

Security is of paramount importance for government mobile applications as they often handle sensitive data and facilitate critical services for citizens. Ensuring robust security measures, such as encryption, authentication mechanisms, and regular audits, is essential to safeguard against cyber threats and data breaches. By prioritizing security, government institutions can protect the confidentiality and integrity of user information, maintain public trust, and uphold the credibility of their services. Additionally, strong security practices mitigate the risk of unauthorized access or manipulation of government systems, thereby safeguarding national interests.

Government institutions should follow RISA software security and data privacy guidelines when designing mobile applications. In particular, the following guidelines should be followed for mobile applications:

Security

Least privileges [Mandatory]

Mobile applications should be designed with the least privileges on the device that it is installed on. For example, write access to the devices data store should not be sought unless it is essential for the mobile app to perform its functions.

Secure coding practices [Mandatory]

Follow secure coding best practices, such as input validation, parameterized queries, and output encoding, to prevent common vulnerabilities like SQL injection and cross-site scripting (XSS)

Multi-factor Authentication [Mandatory]

Multi-Factor Authentication (MFA) is strongly recommended as the primary authentication method for government institutions in Rwanda. It provides a high level of security by requiring users to present multiple independent factors for identity verification, significantly reducing the risk of unauthorized access

Session handling [Mandatory]

Session handling requires appropriate controls to be placed on the backend server to which the application connects. The backend server should treat the application as an untrusted entity; only allowing it access to content that it has been authorised to. When an application has authenticated, the backend server should enforce a session timeout, after which the application is forced to re-authenticate.

Sensitive data storage [Mandatory]

Sensitive information should not be stored on a device when it is not required. When sensitive data is required to be stored on a device, developers should look to make use of any native protected data storage APIs that are available to the platform. When it is no longer required on the device, it should be securely removed.

Encryption [Mandatory]

- Implement encryption algorithms to protect sensitive data both in transit and at rest. Use industry-standard encryption algorithms like AES (Advanced Encryption Standard) to secure user data
- Storing any cryptographic keys on the device will reduce the effectiveness of an additional cryptographic layer as keys stored locally could be recovered from the device (though these keys could be combined with a user credential to strengthen them). Storing the keys on a remote server would prevent an attacker with physical access to the device

from retrieving them, though would require the application to authenticate to the server, and have an internet connection.

- Encrypt sensitive data stored on the device, such as user credentials, personal information, and payment details. Apply encryption to local databases or use secure key storage mechanisms provided by the mobile operating system

Security audits [Mandatory]

Conduct regular security audits and penetration testing to identify vulnerabilities and address them promptly

Security updates [Mandatory]

Stay updated with the latest security patches and updates for the mobile operating system, libraries, and frameworks used in the app

Data privacy

Ensuring data privacy for government applications in Rwanda is crucial to complying with Rwanda's law on the protection of personal data and privacy. Adhering to these regulations is not only a legal obligation but also a means to uphold citizens' fundamental rights and trust in government services. By safeguarding the privacy of personal data, government applications can mitigate the risk of unauthorized access, misuse, or disclosure of sensitive information. This fosters a culture of accountability and transparency, reinforcing citizens' confidence in the government's commitment to respecting their privacy rights. Government institutions should follow RISA's privacy by design guidelines when developing mobile applications. Key considerations include:

Notice on personal data collection [Mandatory]

Mobile application users should be given clear, specific and complete notice on how a government institution will use and disclose personal information collected by the mobile app, including the device features the app requests access to and the reasons for seeking these permissions. Clearly communicate to users how their data will be collected, used, and shared through a privacy policy or disclosure statement.

Consent for data collection [Mandatory]

Obtain informed consent from users before collecting and processing their personal information.

Minimal data collection [Mandatory]

Minimize the collection and retention of personally identifiable information to reduce the potential impact of a data breach.

Data anonymisation [Mandatory]

Implement data anonymization techniques whenever possible to protect user privacy.

Privacy guidelines [Mandatory]

Ensure compliance with RISA privacy by design guidelines and Rwanda's Data Protection Law.

Maintenance of mobile applications

Maintenance of mobile applications is a critical activity to ensure their continued functionality, usability and security. Key guidelines include:

Monitoring analytics [Mandatory]

Government institutions should apply appropriate analytics tools for monitoring the mobile app to gauge user engagement and behaviour. This will facilitate continuous improvement. At the very least, platform analytics should be reported through Apple iTunes Connect (iOS) and Google App Analytics (Android). Analytics should report how many potential users visited the app store promotion pages, how many downloaded the app, and the user rating on the App Store and Google Play.

Maintenance of mobile applications

User support and feedback[Mandatory]

Provide options for users support and feedback within the mobile app where possible.

Maintenance of mobile applications

Compatibility to new device versions and software[Mandatory]

Continuously assess compatibility of the app to new versions of Operating systems e.g IOS or Android as well as new versions of mobile devices.

Maintenance of mobile applications

Regular updates[Mandatory]

Monitor the application regularly to check for issues and bugs which should be resolved on a timely basis to ensure continued user satisfaction. Regular updates must be provided to address bugs, enhance features, and adapt to evolving technology standards.

Maintenance of mobile applications

Security maintenance[Mandatory]

Regular security audits are essential to protect sensitive government data and maintain public trust. Regular security updates should be done to address any security issues identified.

Maintenance of mobile applications

Performance monitoring[Mandatory]

Monitor the application's performance. Check the speed, friction in usage and load times for the application and make improvements as required so ensure a smooth user experience.