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
- Data privacy

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.