Standards

*Some general coding best practices relevant to mobile coding:*

• Input Validation and Output Encoding

• Minimise lines of code.

• Use safe languages (e.g. from buffer-overflow).

• Implement a security report handling point (address) security@example.com

• Use static and binary code analyzers to find security flaws.

• Use safe string functions, avoid buffer and Integer overflow.

• Run with the minimum privilege required for the application on the operating system.

• Be aware of privileges granted by default by API's and disable them.

• Don't authorize code/app to execute with root/sa privilege.

• Always perform testing as a standard as well as a privileged user.

• Avoid opening application specific server sockets (listener ports) on the client device.

• Use the communication mechanisms provided by the OS.

• Context aware security: may be able to decrease/increase access based on the context (e.g. location, network).

• Remove all test code before releasing the application.

• Ensure logging is done appropriately but do not record excessive logs, especially including sensitive user information.

• What sort of information should be recorded in the logs. (Keep audit data on the server, no user specific data - link to the Apple Issue - Signed Timestamps).

References

https://github.com/NormanChiflen/Continuous-Integration--QA-Test--Deploy---Feedback/wiki/Coding-standards-for-mobile-apps