Standard

Mobile Application & Operating Systems Standard

HPRM:19/227306

Implementation Date: 1 July 2019

Version: 2.0

Audience

- Department-wide[1]
- Technical and business professionals, and service partners who participate in the design, development, maintenance and support of IT solutions.
- Project managers, business analysts or anyone involved during portfolio and project planning, conducting impact assessments or requirements analysis activities.

Purpose

This document details the Department of Education mobile application development and mobile operating system standard. Supported mobile operating systems and versions are declared along with mobile application development standards, which ensures that the department develops applications that are secure by design and industry supported secure mobile operating systems.

1 Scope

The following items are within the scope of this standard:

- Resources consumed by the Department of Education to support, maintain or update mobile applications as a result of:
  - Procurement of ICT services
  - ICT Development Projects
- External developers or vendors developing mobile applications for, or on behalf of, the Department of Education.

Out of Scope Software-as-a-Service based mobile applications developed by vendors or government agencies whom will fully support and maintain the application are out of scope of this standard.

2 Handling of Exemptions

- Any exemption to this standard could be subject to CIO approval.
- All exemptions require approval by the Domain Architecture and Standards Group.

3 Standard Exceptions

Microsoft Windows Mobile The department has stopped further development efforts for Microsoft Windows Mobile and is retiring this platform and existing departmental applications must be supported until the application is removed from the Windows Store.

[1] Including but not limited to includes schools, divisions, units, offices, and business units

4 Mobile Operating Systems

4.1 Apple iOS

Apple iOS must be supported for the current and previous three `MAJOR` versions.

> Determining the supported version is calculated as as follows `N` minus `3` version support where `N` is the `MAJOR` version number[2].

4.2 Google Android

Google Android must be supported for the current and previous five `MAJOR` versions.

> Determining the supported version is calculated as as follows `N` minus `5` version support where `N` is the `MAJOR` version number[3].

5 Early Withdrawal of Support

Early withdrawal of support is where the department should immediately stop support and development for mobile operating systems where the developer or vendor has withdrawn support due to security or compatibility reasons; for example:

- Spectre and Meltdown[1]

[2] See Section 6.2
[3] See Section 6.2

6 Mobile Application Development

6.1 Security

Mobile application developers must follow security or development best practices in the following order of priority:

1. Latest Information Management and Information Security standards and processes specified by the department.
2. Latest departmental application development best practices and standards.
3. Latest mobile operating system development, security guidelines and best practices available; for example:
    - NIST 800-163 Vetting the Security of Mobile Applications[2].
    - OWASP Mobile Security Testing Guide [3].

6.2 Version Numbering

Development of mobile applications must adhere to `MAJOR.MINOR.PATCH` semantic versioning[4].

6.2.1 Versioning Guidance

The first version of an mobile application must always start with a `MAJOR` version of 1 and should use the following guidelines when incrementing version numbers:

- `MAJOR` version when you make incompatible or breaking changes
- `MINOR` version when you add functionality in a backwards-compatible manner
- `PATCH` version when you make backwards-compatible bug fixes.

Legislation

Nil

Related Policies

Nil

Related Procedures

Nil

Related Standards

- Semantic Versioning [4]
- NIST 800-163 Vetting the Security of Mobile Applications [2]

Guidelines

Nil

Supporting Information/Websites

- OWASP Mobile Security Testing Guide [3]
- ACSC - Update on processor vulnerabilities (Meltdown/Spectre)[1]

Contact

For further information, please contact:

Mobile Application Development

- email: DL-ITBMobileApplications@qed.qld.gov.au

Cyber Security

- email: operational.security@qed.qld.gov.au
- Intranet site (DoE employees only): https://intranet.qed.qld.gov.au/Services/InformationTechnology/ict-policy-security/

Information & Governance Management

- email: InformationManagement@qed.qld.gov.au
- Intranet site (DoE employees only): https://intranet.qed.qld.gov.au/Services/InformationTechnology/information-management/information-management-toolkit/

Review Date

Next Review Date: 1 July 2021

Creative Commons Licence

Superseded Versions

Application Development Mobile Operating Systems Standard - Version 1.0

References

[1] *Update on processor vulnerabilities (Meltdown/Spectre)*. ACSC Report. Australian Cyber Security Centre, 2018. URL: https://www.cyber.gov.au/news/update-on-processor-vulnerabilities-spectre-meltdown.

[2] *NIST Special Publication 800-163 Revision 1 - Vetting the Security of Mobile Applications*. NIST Standard. HPRM: 20/398881. National Institute of Standards and Technology, 2019. URL: https://doi.org/10.6028/NIST.SP.800-163r1.

[3] *OWASP Mobile Security Testing Guide*. OWASP Guide. Open Web Application Security Project, 2020. URL: https://owasp.org/www-project-mobile-security-testing-guide/.

[4] *Semantic Versioning*. Industry Standard. Tom Preston-Werner, 2018. URL: https://semver.org/.