
SOK Development Guidelines

A handbook created by developers for developers to help engineering teams to align their software practices and share know-how.

Development Community



2020-10-02

This is a high-level document containing a collection of best practices, commonalities between projects and values proven to be practical. Team's should follow these guidelines when implementing their software.

Contents

Codebase	3
Version Control	3
Branching	3
Coding Standards	3
Mobile Development	4
Environments	4
Data	4
Mobile Development	4
Design	4
Architecture	4
Infrastructure	4
Security	4
Guidance	4
Documentation	4

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119.

Codebase

Version Control

- MUST use version control
- SHOULD use Git
- MUST use `master` branch as a base for development
- MUST have documented version control flow

Branching

- MUST fork feature (and release) branches from `master` branch
- SHOULD protect default branch from pushes

Mobile development

- SHOULD use fast-forward merges only from feature branch to `master` branch
- SHOULD implement bug fixes to feature branch and cherry picked them to `master` and potential release branch
- RECOMMENDED to squash feature branches before merging to `master` branch
- MUST preserve release tags forever

Coding Standards

- MUST agree on a coding standard inside a team # Release Management
- SHOULD release to production from branch that's used for base of development
- MUST have identifiable releases
- RECOMMENDED to release smaller changes often over larger merges
- MUST have (at least) following stages in pipeline (in recommended order): install, test, scan, build, deploy, verify, release

Mobile Development

- MUST use semantic versioning for releases (tags)

Environments

Data

Mobile Development

- SHOULD preserve all release artefacts forever

Design

- SHOULD name AWS profiles after account-aliases

Architecture

Infrastructure

- SHOULD use semantic versioned Docker images for building releases

Security

- MUST run automated vulnerability checks for code
- SHOULD run automated static code analysis for code quality

Guidance

- MUST have process how to handle security notifications

Documentation

- SHOULD use README.md as a central information document inside code repository
- SHOULD document all exceptions with reasoning from Development Guidelines in project's README.md