Policy Contact	Roberto Cordero: Cordero.r.3@pg.com	Revised Date	October 16th, 2024
	Gil Bautista: bautista.gz@pg.com		
	RJ Winkler: winkler.rj@pg.com		

Software Development Lifecycle (SDLC) Document for P&G Suppliers

1. Document Purpose

The purpose of this Software Development Lifecycle (SDLC) document is to ensure software development in P&G meets functional, non-functional, regulatory, and security requirements and leverages industry standards and best practices.

This will enable P&G to meet business needs with quality, security, and long-term maintainability. Utilizing a disciplined, structured process helps to ensure that quality and security are planned, built-in, and deployed as an integral part of the software development lifecycle.

2. Scope

This document applies to all organizations, and individuals, **including third party partners or suppliers**, who develop and/or modify software used individually or **in support of P&G business** processes.

The P&G SDLC process includes the following:

1. **People & Culture:**
   Software products are identified and mapped to a Product Team.

2. **Plan & Develop:**
   Software requirements and design are documented.
   Software source code is stored and secured properly.

3. **Build & Test:**
   Security is embedded early and throughout the software lifecycle.
   Software is tested is according to the company's Service Validation and Testing policy.

4. **Release & Deploy:**
   Software is deployed according to the company's IT Change Management policy.

5. **Operate, Observe, & Respond:**
   IT Service Management processes (such as Incident Management, Problem Management) are done according to the company's ITSM procedures.

Policy Contact	Roberto Cordero: Cordero.r.3@pg.com	Revised Date	October 16th, 2024
	Gil Bautista: bautista.gz@pg.com		
	RJ Winkler: winkler.rj@pg.com		

3. Requirements

All software development and/or modification must follow a well-documented and repeatable Software Development Lifecycle (SDLC) process. The SDLC should have control points where quality, security, and long-term maintainability considerations are evaluated and determine whether development can progress or further improvements and/or remediations are required.

- Architecture Environment Diagram and Technical Infrastructure Diagram of the software must be stored in company's approved Enterprise Architecture Artifact Repository.
- Software source code owned by P&G must be stored in a P&G approved source code management system.
- Actor verification: every change in the revision's history must have at least one verified actor identity (author, uploader, reviewer).
- History retention: codebase revisions and change history must be preserved indefinitely and cannot be deleted, except when subject to an established and transparent policy for obliteration, such as removal of secrets or to meet legal and/or policy requirements.
- Two-person revision: Every change to source code must have an authorized author and an authorized reviewer. These must not be the same authorized individual.
- Software source code repository(ies) must be mapped to the software registered in the P&G approved IT Asset Management system.
- Static Application Security Testing (SAST) must be applied during development cycle to detect inner-made software vulnerabilities.
- Software Composition Analysis (SCA) must be applied during the development cycle to detect open-source vulnerabilities.
- Code quality scanning must be applied during the development cycle to detect bugs and code smells.
- All components of each software release must be recorded and shared through software bill of materials (SBOM).
- Credentials (passwords, access tokens and keys) must not be hardcoded in any repository.

4. Compliance

4.1. Compliance Measurement

The P&G Software Development Lifecycle Policy team will verify compliance through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. Exceptions

Any exception to the policy must use the established IT Compliance Exceptions Process.

4.3. Non-Compliance

Violating this Policy may result in disciplinary action, consistent with local laws. Employees affected by this are expected to read and follow it, directing any questions to the Policy Contact.

5. Appendix or References

5.1. Related Standards, Policies and Processes

NIST SP 800-218 Secure Software Development Framework (SSDF)
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf

Supply-chain Levels for Software Artifacts (SLSA)
https://slsa.dev/