PKCERT

National Cyber Emergency Response Team
Government of Pakistan

Pakistan Information Security Framework (PISF) 2025

ESSENTIAL SECURE SOFTWARE DEVELOPMENT LIFE CYCLE (SSDLC) CONTROLS

NTISB

A. INTRODUCTION

1. Pakistan Information security Framework 2025: **"Essential SSDLC Controls"** outlines the baseline of information security SSDLC controls for federal and provincial government ministries, divisions and departments, autonomous bodies, corporations, CERTs and designated CIIs.

2. This framework applies to all individuals and entities involved in the development, acquisition, deployment, and maintenance of software and applications. It covers all types of applications and environments, ensuring that security controls are systematically integrated throughout every phase of the software life cycle to protect personal, sensitive, and business-critical data in compliance with national cybersecurity regulations and standards.

B. SSDLC CONTROLS

3. All those organizations involved in software development for other organizations or for internal use shall ensure that requirements for SSDLC shall be defined, documented, approved and implemented.

4. The requirements for SSDLC shall have but not limited to the following: -

a) Embed security from the earliest stages of software development and ensure alignment with well-known standards.

b) Security integrated throughout the SDLC, from defining requirements through risk and compliance inputs to secure design, coding, testing, and deployment.

c) Security validation of code before release, with post-implementation reviews.

d) Appropriate training for developers in secure coding practices.

e) Separate development, testing, and production environments.

f) Maintain secure repositories for source code and configuration items.

g) Security review and approval for all commercial, open-source, and third-party components (software libraries, modules, middleware, etc.) before acquisition and integration.

h) Adoption of approved tools for code scanning, security testing, dependency management, and version control, integrated into the CI/CD pipeline.

i) Comprehensive testing through expert code reviews and manual/automated assessments of all software and applications.

j) The organization shall ensure that appropriate third-party security testing is performed for software as part of the secure development and acquisition lifecycle.

PKCERT

Safeguarding Pakistan's Cyberspace

info@pkcert.gov.pk
www.pkcert.gov.pk