piksel mutfak

PXL Digital Solutions

Secure SDLC Policy

DOCUMENT CONTROL	
1 **Version:**	2.1.5
2 **Effective Date:**	16 February 2027
3 **Owner:**	PXL Digital Solutions Management
4 **Classification:**	Internal
5 **Review Cycle:**	Annual
6 **Approved By:**	Management

1. Purpose

The purpose of this Secure Software Development Life Cycle (SDLC) Policy is to establish mandatory security principles and controls for the planning, design, development, testing, deployment, maintenance, and retirement of software developed or managed by PXL Digital Solutions.

2. Scope

- Applies to employees, contractors, consultants, and third parties involved in software delivery.
- Covers web, mobile, backend, API, cloud, automation, AI-enabled, and internal business applications.
- Applies to new development, enhancements, integrations, maintenance, configuration changes, and decommissioning activities.
- Covers source code, infrastructure-as-code, scripts, libraries, build pipelines, test assets, and deployment configurations.

3. Secure Development Objectives

- Integrate security throughout the software lifecycle rather than treating it as a final-stage activity.
- Reduce vulnerabilities through secure design, coding, testing, and change management practices.
- Protect customer data, credentials, source code, intellectual property, and production services.
- Ensure identified security risks are documented, prioritized, remediated, or formally accepted.
- Maintain traceability and accountability for material software changes and releases.

piksel mutfak

PXL Digital Solutions

Secure SDLC Policy

4. Roles and Responsibilities

Management:

- Approves this policy, assigns resources, reviews material security risks, and authorizes significant exceptions.

Product and Project Owners:

- Define business and security requirements, identify sensitive data, and ensure security activities are included in plans and acceptance criteria.

Development Team:

- Implements secure design and coding practices, protects secrets, performs peer review, and remediates identified weaknesses.

Technical or Security Lead:

- Supports risk assessment, architecture review, security testing decisions, and escalation of significant findings.

Quality Assurance and Operations:

- Validate release criteria, maintain environment separation, monitor deployments, and support controlled recovery or rollback.

5. Security Requirements and Planning

- Security, privacy, authentication, authorization, logging, availability, and data retention requirements shall be identified during planning.
- Projects handling confidential or restricted information shall include a documented risk review before production use.
- Security requirements shall be included in user stories, specifications, acceptance criteria, or equivalent project records.
- Material changes to data flows, integrations, privileges, or trust boundaries shall trigger reassessment.

6. Secure Design and Architecture

- Designs shall apply least privilege, defense in depth, secure defaults, and separation of duties where practical.
- Trust boundaries, data flows, external integrations, abuse cases, and failure modes shall be considered for higher-risk systems.
- Approved cryptographic mechanisms and secure transport shall be used for sensitive information.
- Administrative interfaces and high-risk functions shall receive enhanced authentication, authorization, and audit controls.

7. Secure Coding Standards

- Developers shall follow recognized secure coding guidance appropriate to the technology stack, including awareness of common web and API risks.
- Input validation, output encoding, authorization checks, secure error handling, and safe file processing shall be implemented where applicable.
- Credentials, tokens, private keys, and secrets shall not be embedded in source code or client-side applications.
- Security-relevant events shall be logged without recording unnecessary sensitive data or plaintext secrets.

piksel mutfak

PXL Digital Solutions

Secure SDLC Policy

8. Source Code Management

- Source code shall be stored in approved version-control repositories with unique user access and role-based permissions.
- Material changes shall be traceable to an authorized request, issue, or business requirement.
- Peer review shall be performed for significant changes before production release whenever practical.
- Protected branches, review controls, and repository backups shall be used according to project risk.

9. Third-Party Components and Dependencies

- Libraries, packages, SDKs, containers, and external services shall be obtained from trusted sources and used only when justified.
- Known vulnerabilities, maintenance status, licensing, and supplier risk shall be considered before adoption.
- Dependency versions shall be tracked and updated based on security risk and compatibility.
- Unsupported or materially vulnerable components shall be replaced, remediated, isolated, or covered by an approved exception.

10. Secrets and Configuration Management

- Secrets shall be stored in approved secret-management or protected configuration mechanisms and restricted to authorized identities.
- Development, test, and production credentials shall be separated, and production secrets shall not be used in lower environments.
- Configuration values shall follow secure defaults and shall be reviewed before release.
- Compromised or exposed secrets shall be revoked or rotated without unnecessary delay.

11. Security Testing

- Testing shall be risk-based and may include code review, static analysis, dependency scanning, dynamic testing, API testing, configuration review, and manual security testing.
- Critical authentication, authorization, data validation, and administrative workflows shall receive focused negative and misuse testing.
- Security findings shall be recorded with severity, affected asset, owner, remediation action, and status.
- Independent vulnerability assessment or penetration testing shall be considered for internet-facing or high-risk systems.

piksel mutfak

PXL Digital Solutions

Secure SDLC Policy

12. CI/CD and Release Management

- Build and deployment pipelines shall use controlled access, protected credentials, and traceable execution records.
- Security checks appropriate to project risk shall be included before release, and failed mandatory checks shall block or escalate deployment.
- Release packages shall be generated from approved source and deployed using controlled procedures.
- Rollback or recovery procedures shall be available for material production releases.

13. Environment Separation and Change Control

- Development, test, staging, and production environments shall be logically separated according to risk.
- Production access and deployment permissions shall be limited to authorized personnel.
- Customer or production data shall not be copied to lower environments unless authorized and appropriately protected.
- Emergency changes shall be documented and reviewed after implementation.

14. Vulnerability Remediation

Security findings shall be prioritized according to severity, exploitability, exposure, affected data, and business impact. Target remediation periods apply unless a documented exception or risk acceptance is approved.

Severity	Required Action	Target
Critical	Immediate containment and prioritized remediation	7 days
High	Prompt remediation and management tracking	30 days
Medium	Scheduled remediation based on risk and exposure	90 days
Low	Planned remediation or documented risk acceptance	180 days

piksel mutfak

PXL Digital Solutions

Secure SDLC Policy

15. Data Protection and Privacy

- Applications shall collect, process, transmit, and retain only the information required for authorized business purposes.
- Sensitive information shall be protected in transit and at rest where appropriate to risk and contractual requirements.
- Test data shall be synthetic, anonymized, masked, or otherwise protected whenever practical.
- Customer data shall not be submitted to third-party AI or external processing services unless approved and contractually permitted.

16. Logging and Monitoring

- Applications shall generate sufficient logs to support troubleshooting, security monitoring, incident investigation, and accountability.
- Logs shall protect sensitive data, use appropriate access controls, and be retained according to business and contractual requirements.
- Security-relevant failures, suspicious activity, and significant administrative actions shall be monitored where practical.

17. Security Exceptions

Exceptions to this policy shall be documented with the business justification, affected systems, risk assessment, compensating controls, owner, approval, and expiry or review date. Exceptions shall not be treated as permanent unless formally renewed.

18. Training and Awareness

Personnel involved in software delivery shall receive security awareness appropriate to their responsibilities. Developers and reviewers should receive periodic guidance on secure coding, dependency risk, secrets handling, and attack patterns relevant to the technologies they use.

piksel mutfak

PXL Digital Solutions

Secure SDLC Policy

19. Compliance and Records

PXL Digital Solutions aims to develop and operate software in accordance with applicable legal, contractual, regulatory, and customer-specific security requirements. Reviews, test results, approvals, exceptions, and remediation records shall be retained as appropriate.

20. Policy Review

- Reviewed at least annually
- Reviewed following significant security incidents or material software delivery changes
- Updated when legal, contractual, regulatory, or technology requirements materially change
- Latest approved version shall be made available to relevant personnel

APPROVAL & ACKNOWLEDGEMENT

Approved By: _____

Title: _____

Signature: _____

Date: _____

This document is intended for internal use and customer assurance purposes.