PDS INFOTECH PVT LTD

Secure Development Policy

Ref No: ISMS/PDS/5.2/8.1

1. Purpose

PDS Infotech Pvt Ltd ("the Company") develops ready-to-use software products, primarily around business process automation. This policy defines the controls the Company applies across the software development lifecycle to ensure that products are designed, built, tested, and released securely.

2. Scope

This policy applies to all software development activity conducted by or on behalf of the Company, including internally developed products and any development work performed by third-party or outsourced developers.

3. Policy

3.1 Coding Guidelines

- Developers must follow the Company's documented secure coding guidelines, informed by recognized industry standards for the languages and frameworks in use.
- Secure coding guidelines must address common vulnerability classes relevant to the Company's technology stack, including injection issues, broken authentication, and improper access control.
- Coding guidelines must be reviewed and updated at least annually, or when a significant new vulnerability class or technology is adopted.

3.2 Code Repositories and Reuse

- All source code must be maintained in an approved, access-controlled version control repository.
- Reuse of existing code, internal libraries, and repositories is encouraged to reduce duplicated effort.
- Third-party libraries, packages, and open-source components must be vetted before use, including a check for known vulnerabilities and license compatibility.
- Direct commits to production release branches without review are not permitted.

3.3 Code Review and Approval

- All code changes must undergo peer review by a developer other than the author before being merged into a shared or release branch.
- Code review must check for adherence to secure coding guidelines, correctness, and maintainability, in addition to functional correctness.
- Formal approval by a designated reviewer or lead is required before code is merged and before a release is built for deployment.

3.4 Separation of Environments

- Development, testing/staging, and production environments must be logically or physically separated, with distinct access controls for each.
- Production data must not be used in development or testing environments unless it has first been anonymized or masked.

- Access to the production environment must be restricted to authorized personnel and must be logged.

3.5 Testing

- Testing scripts must be prepared and maintained for each module/sub-module, covering functional correctness and, where applicable, security-relevant test cases.
- Test data must be synthetic or masked. Production data containing personal data, as defined under the Digital Personal Data Protection Act, 2023, or Client Confidential Data must not be used in test environments unless anonymized to remove identifying or sensitive content.
- Where use of production-derived data in testing is unavoidable for a specific, documented reason, it must be approved in advance by the Information Security team and subject to the same protections as production data.

3.6 Security Testing and Penetration Testing

- An external penetration test must be conducted at least annually. Findings must be risk-rated, and remediation timelines must be assigned based on severity, with critical findings remediated on a priority basis.
- Retesting must be conducted to confirm remediation of critical use cases.

3.7 Outsourced Development

- Where development work is outsourced to a third party, the engagement must be governed by an agreement addressing secure coding requirements, code ownership, confidentiality, and the Company's right to review or audit the delivered code.
- Code delivered by outsourced developers is subject to the same code review, testing, and security testing requirements as internally developed code before release.

3.8 Change Management

Changes to production systems must follow a documented change management process, including testing, approval, and a rollback plan, before deployment.

4. Roles and Responsibilities

- Development Team: Follow secure coding guidelines, participate in code review, and maintain test scripts.
- Development Leads/Managers: Approve code changes and releases.
- IT Management: Maintain environment separation and manage access to production systems.

5. Review

This policy shall be reviewed at least annually, or upon significant technological or regulatory change, to ensure continued alignment with ISO/IEC 27001:2022.