DSP
ASSET MANAGERS

Secure Development Life Cycle Procedure

Document Control	
Document Title: Secure Development Life Cycle Procedure	Version: 2.0
Document Owner: Chief Information Security Officer	Effective Date: February 2025
Location: Intranet	Review Frequency: Annually
Department: Information Technology	

Version History					
Version	**Date**	**Summary of Change**	**Author**	**Reviewer**	**Approver**
V 1.0	Feb 2024	New Document	Bhushan Somvanshi (AVP)	Nikhil Sharma (Sr. Mgr.)	Fal Ghancha (CISO)
V 1.1	Sept 2024	Reframed certain procedure statements in section 6.1, 6.3, 6.5, 6.6 & 6.10	Bhushan Somvanshi (AVP)	Vimal Ahir (AVP)	Yogesh Bhalla (CTO)
V 2.0	Feb 2025	Modified Clause 6.1, 6.2 & 6.6	Bhushan Somvanshi (AVP)	Vimal Ahir (AVP)	Hiren Pandya (CISO)

Table of Contents

1. Introduction

This procedure provides the information security requirements related to information systems and applications during the entire lifecycle of software development for DSP Asset Managers Private Limited (hereby referred to as "DSPAM").

2. Scope

This procedure covers all DSPAM Information Technology (IT) services, systems and information assets. This procedure applies to all DSPAM employees and contractors (including consultants and Third-party personnel) who are directly or in-directly employed by DSPAM (henceforth referred to as "users") and authorised to access DSPAM Information assets.

3. Purpose

The purpose of this procedure is to define the minimum-security requirements for in-house developed applications and to ensure that any software development conducted by DSPAM or a third-party provider is secured and reviewed to protect against the exploitation of security gaps.

4. Exception

Any exception to this procedure shall be driven by the Exception Management Procedure. Any exception beyond the exception management procedure shall be as per CISO, CTO and Business Heads' approval. All exceptions granted shall be subject to a procedure waiver for a defined period.

5. Roles and Responsibilities

Roles	Responsibilities
Application team	• Classify applications as per criticality • Develop applications and ensure essential tests are conducted before deploying in production • Resolve vulnerabilities to the application if any • Perform implementation, testing, maintenance, decommission
Application owner	• Provide role based access to the application team • Assist application team in creation of implementation plans • Ensure application team is trained for the secure development • Provide clearance for deploying application in production environment • Raise risk acceptance
Information security team	• Perform vulnerability assessment of the applications • Track with the application team for closure of the identified vulnerabilities

CTO / CISO	• Approve exception and risk acceptance

6. Procedure Description

6.1 General requirements

Application development team / Dev-ops team (here referred to as “application team”) should ensure that all applications of DSPAM are classified as per defined classification scheme within DSPAM and appropriate security controls are implemented to mitigate any identified risks.

Dedicated test systems and production systems should be available and should be implemented on a separate VLAN segment.

For secure rollout of software and applications, threat modelling and application security testing shall be conducted during development.

The principle of defence-in-depth should be adopted to provide a layered security mechanism.

Before introducing new technologies for critical systems, DSPAM shall ensure that IT/ security team has assessed evolving security concerns and achieved fair level of maturity with such technologies before incorporating them into IT infrastructure.

Data Transfer should not be allowed from production system to test system, unless approved by the Application Owner.

Limited users should be provided with privileged access to software (acquired / developed). In case of a specific requirement, access should be granted only for a specific period of time and should be revoked immediately after the time duration is complete.

All critical software/applications should go through appropriate quality testing before deploying in production environment and security assurance testing post deployment in production environment.

Any critical gaps/issues identified during the quality testing that pose a severe security risk to the application should be remedied as per organisational policy.

In case of any major changes to the application that needs to be directly deployed in the production and necessary risk mitigating controls should be implemented and exception approval (if required) should be requested from the application owner and the CTO.

Application team should use secure programming practices as defined in the Secure Coding guidelines.

Any critical internet facing application in case of major architectural change should be reviewed and/or tested for vulnerabilities before it is used in a production environment by the information security team.

For vendor-developed applications, ensure that they are free from critical security vulnerabilities and that their source code complies with industry best practices. Obtain confirmation of these security aspects from the vendors. Additionally, henceforth all manage agreements with the vendor shall be in accordance with the Information Security Vendor Management framework.

6.2 Software application

Critical assets defined as per the Critical Asset Identification and Classification Procedure should have necessary risk mitigation controls implemented to avoid the risk of compromise.

Application owner should ensure that role-based access is provided to the users to perform their duties.

All software applications should be reviewed at least once annually.

Personal Information and sensitive data should be protected whilst in storage and in transmission using appropriate cryptographic controls defined in the cryptography standard.

Critical websites that need to be strongly authenticated, should use SSL certificates provided from a Certificate Service Provider (CSP).

Application team should be responsible to identify and address the security requirement for the application (new /developed) based on the applicable threats and vulnerabilities.

Access to mobile and web applications shall be provided to a customer only at their option, based on a specific written or authenticated electronic requisition, along with a positive acknowledgment of the terms and conditions.

6.3 Software development

The Application Team, in collaboration with Application Owners, should develop implementation plans that align with industry standards, organizational policies, and security requirements.

Application team should design and validate security testing plans, both for development and production stages. Development of the application should be done in consideration with requirements stated in the Secure Coding guidelines.

Source Code of the applications developed in-house should be maintained and stored safely by application team in consultation with the application owner.

6.4 Implementation and review

Application team should ensure development is completed in secured environments. Information security team should establish security-related vulnerability tracking capabilities/resolution paths.

Application owners should ensure development team members are trained on the secure software development.

6.5 Testing/Deployment (User acceptance test)

Application team should ensure that configuration and code reviews (as appropriate) are performed.

Application team should perform all established testing procedures and evaluate gaps in testing.

Application team in co-ordination with the Information security team should conduct preliminary vulnerability tests for their critical application.

Change management procedure should be followed for deploying in production environment.

Same access control procedures should be applied to test environments as those applied to operational environments.

6.6 Maintenance/ Ongoing operations (Production)

Application team should conduct routine security activities, including but not limited to:

- Perform regular backups of sensitive and critical data
- Regression testing shall be undertaken before new or modified systems are implemented. The scope of tests shall cover business logic, security controls and system performance under various stress-load scenarios, and recovery conditions.
- Conduct periodic risk assessments in consultation with information security team
- Conduct periodic training and awareness for internal users of the software, as applicable.

Application team in consultation with the application owner should review functionality and controls, including but not limited to:

- Ensure both automatic and manual security controls are in effect and actively deployed.
- All applications shall be integrated into the SOC to ensure that alerts and notifications are generated effectively, and that an audit trail is maintained.
- Validate training and awareness practices are received and tested routinely.

6.7 Disposal/Decommission

Application team shall ensure change management procedure is followed for decommissioning of the system. Application team shall ensure essential backup of the system or application is taken prior to disposing or decommissioning. The data in the system or application shall be purged to prevent its retrieval or reconstruction.

6.8 Lifecycle phase transition

Prior to a transition to any phase, all items in the previous phase should be either completed, removed, or otherwise accepted by application owner and the application team. Any phase transition without previous phase completion should be halted and regressed immediately, until requirements are met or controlled.

6.9 Security assessment

All critical applications should undergo security assessment and should require clearance from application owner before the application is deployed in production environment.

Once the application is available in production environment, the same should be scoped in as part of Vulnerability Assessment.

Necessary controls should be implemented for the vulnerabilities identified by the application team as applicable.

In the event, that risk cannot be treated, the risk acceptance process should be initiated. Application owner should present the risks to the CTO and CISO for approval.

All the open security issues should be tracked by the application team and information security team for closure.

6.10 Data Protection

When a system or software asset is not in the Maintenance/Ongoing Operations (Production) phase, the system or asset should consider all security measures containing or having references to any live data sets, including those containing non-confidential information – all systems not in production environment should use development data sets, or none at all.

7. RACI Matrix for Secure Development Life Cycle

Sr. No.	Procedure Steps	Application team	Application owner	InfoSec team	CTO/ CISO
1	Classify applications based on criticality	R, A	C	I	I
2	Develop, test, implement, decommission applications	R, A	C	I	I
3	Provide role based access control to the application team, ensure	I	R, A	I	I

Sr. No.	Procedure Steps	Application team	Application owner	InfoSec team	CTO/ CISO
	application team is trained and provide clearance for deployment of application in production				
4	Raise risk acceptance and exception	I	R, A	I	I
5	Perform vulnerability assessment of the applications and track closure of the vulnerabilities	I	A, C	R	I
6	Provide approval for risk acceptance	I	I	I	R, A

RACI Term	Explanation
R (Responsible)	Execute the activity
A (Accountable)	Ensure the activity is executed
C (Consulted)	Contribute to the activity
I (Informed)	Informed about the activity