TRIANZ℠

Secure SDLC Policy

TRIANZ INTERNAL

trianz.com

Statement of Confidentiality

The information contained in this document is internal to Trianz. It shall not be disclosed, duplicated, or used for any purpose other than that stated herein, in whole or in part, without the express written consent of Trianz.

Information Classification

☐	Public
☒	Internal
☐	Confidential
☐	Restricted

Table of Contents

1. Purpose

The purpose of this policy is to establish a process to define security requirements for Software Development Life Cycle for all the projects, products across Trianz.

2. Objective

The objective of Secure SDLC Policy is to: -

- Facilitate efficient implementation of security controls throughout the Development Life Cycle for Trianz managed applications.

3. Scope

The successful implementation of the Secure SDLC Policy requires a consistent and systematic approach to Secure SDLC across Trianz's projects and Products. Scope of the policy is as follows.

- Secure SDLC shall be applicable to all Implementation, Support and Testing projects falling under the applicable Cloud, Analytics, Digitization, Infrastructure Practices and Trianz products and services

This policy applies to all existing and new software developed by Trianz Delivery Teams for internal, external or Client Managed Systems.

4. Policy Statements

Information Security & Data Privacy will be applicable at all stages of the Software Development Life Cycle (i.e., Requirements, Design, Coding, Validation, Release and Response, Maintenance and Decommission)

This policy aims to be language and platform independent so that it is applicable across all software

During all phases of the SDLC where a system is not in production and following conditions are met i.e., the system must not have

a) live data sets that contain information identifying actual people or corporate entities,

b) actual financial data such as account numbers, security codes, routing information,

c) or any other financially identifying data. Information that would be considered sensitive must never be used outside of production environments.

Ensure Security Metrics applicability for improvement of performance at each stage

For each phase of the Development Life Cycle, Trianz Secure SDLC Policy shall ensure the following

4.1 Requirement Phase:

- Ensure conformance with all appropriate security, privacy and compliance requirements by using the Techniques – Security Risk Analysis, Threat Modeling, Use cases/ Abuse Cases
- Ensure CIA triad and authentication, authorization and accountability policies are strictly adhered
- Ensure all development community shall undergo Secure SDLC training (Online or Classroom)
- All applications handling, processing or storing critical or Personal or sensitive data shall follow applicable Data Privacy Guidelines.

- Organization-specific expectations and approved principles for secure coding shall be used for both in-house and outsourced code developments.

4.2 Design Phase:

- Threat Modeling shall carry out to identify potential vulnerabilities, the high-risk interfaces, and any countermeasures
- Ensure planning to meet security and privacy requirements and goals.
- Test Scenarios shall be designed based on Cases/Abuse Cases
- Sensitive information shall be protected throughout its life cycle.
- Shall include Security architecture Design Principles by following Guidelines on Secure System Engineering Principles (e.g., web, applications, user interfaces, programmatic Interfaces, file import/export, reports, and databases).
- Access to source code and other critical system resources during development, testing or production shall be limited to authorized personnel as per Access Control Policy.
- Periodic Secure Architecture Review shall be conducted as per Design Principles by following Guidelines on Secure System Engineering Principles

4.3 Development Phase:

- Secure Coding guidelines shall be followed during the coding
- Security Code Reviews shall be carried out in every code check-in/built.
- Code reviews can be either manual or automated using technologies such as static application security testing (SAST) and Software Composition Analysis (SCA) tools for open-source components.

- Defensive Programming Techniques are applied for coding (wherever applicable)Controls and remediation against the OWASP top 10 vulnerabilities, CWE/SANS Top 25 Programming errors shall be applicable as per Technologies
- Secure coding practices specific to the programming languages and techniques shall be used.

4.4 Validation Phase:

- DAST, SAST, SCA for monitoring third party libraries, Penetration Testing and Vulnerability Testing and Compliance Check shall be carried out during the Validation Phase
- Ensure the backend Network security controls such as DMZ, Network firewall, WAF, IDS/IPS are implemented and reviewed.
- Security findings shall be remediated and managed such as No open critical, High, medium vulnerabilities open in SAST, DAST and VAPT,
- As part of BCP, DRP-All backup and restore mechanisms are in place.
- Testing shall be conducted during and after development. Static application security testing (SAST) processes shall identify security vulnerabilities in software

4.5 Release and Response

- secure deployment and separation of duties shall be practiced.
- Application code for applications shall be reviewed and approved by the Project/Product/Application Architect prior to deployment.

4.6 Maintenance Phase:

- Shall include Change management

- Perform Risk Assessment when the system is modified.
- Ensure all significant changes in application code shall also be reviewed for vulnerabilities prior to deployment.
- The software's shall require regular maintenance and updating, to keep up with changes to common technology, integrations with new tools, and emerging vulnerabilities.
- Code reviews shall be conducted whenever the code is modified/changed
- Periodic vulnerability assessments shall be performed on production /Application Support systems and appropriate measures taken to address the risk associated with identified vulnerabilities.
- Source code shall be protected against unauthorized access and tampering (e.g. by using configuration management tools, which typically provide features such as access control and version control).

4.7 Decommission Phase:

- The data shall be removed securely when the system is retired as per the Data retention policy

5. Roles and Responsibilities:

Roles	Responsibilities	External/Internal
Internal Apps Team	To conduct the necessary scans and provide the reports	Internal

Project Manager / Product Manager	Define the strategy for the appropriate security standards of all software applications handling sensitive information that are accessible from the organization., as well as to monitor, establish and enforce remediation timelines and sanctions for non-compliant systems.	Internal
IS Operations	Perform Vulnerability scan on Application and provide reports	Internal
InfoSec Team	Manage the end-to-end application security assessment Review & follow-up to remediate the VA scan and Code Review report Track the closure report	Internal
CIO/CISO	Review and approve the final assurance report.	Internal

6. Prerequisites

6.1 Training

- CSSLP Training

6.2 Reference Policy, Process, Procedure, Templates, Checklist

Document Name

Secure SDLC Procedure
Access control Policy
Dev Sec Ops Procedure
Vulnerability Assessment and Penetration Testing Procedure
Information Security Assessment Checklist
Cloud Security Privacy Policy
Patch Management Policy
Incident management procedure
Risk and Opportunity Management Procedure

7. Standards Addressed

Standards Covered
ISO 27001:2022-ISMS (Information Security Management System) ISO 27701:2019-PIMS (Privacy Information Management System)

8. ISO Control/Clause Mapping

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
Technical Control	Clause 8.27 Secure System Architecture and Engineering Principles	Secure SDLC policy
Technical Control	8.25 Secure development life cycle Control Rules for the secure development of	Secure SDLC policy

	software and systems shall be established and applied. Clause 8.28 Secure Coding	
Technical Control	8.29 Security testing in development and acceptance	

9. Exceptions(s)

- Exceptions require a documented business justification. Exceptions are subject to the approval of CIO/CISO
- Requests for exceptions of medium and low risk issues may only be made by an agency's Information Security Officer (ISO) or application's business owner.

Document Control

Owner:	CISO	**Release ID:**	SSDLC-POL-046

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver.No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.00	16-Sept-11	Srilakshmi	-	-	Initial Version	None
1.00	23-Sept-11	Srilakshmi	-	-	Request for Baseline	Baselined
2.00	23-Jul-12	Srilakshmi	-	-	Logo change and replaced revision with version	Modified logo and replaced revision with version
3.00	12-Nov-14	Srilakshmi	-	-	PCR raised by Deb	Added classification of the document as 'Internal Use Only' in the footer of the document Removed Information classification and Table of contents Removed Release ID in the header Modified logo

3.01	28-Nov-7	Sudharsana	Vijaya	-	For QMS Upgrade against PCR 24	PCR 24- for updates in Revision History i.e. adding Reviewer and Approver columns Adding Pilot Release Date and Effective Date in Document control Information
4,00	28-Nov-17	Sudharsana	Vijaya	Ganesh	For QMS Upgrade against PCR 24 and approval	Approved
5.00	10-Dec-18	Vijaya	Balu	Ganesh	Information classification updated	Approved and Baselined
6.00	2-Nov-19	Vijaya	Information Security Team	Vivek	Periodic Review & Update	Reviewed and Approved
6.01	30-Dec-20	Divya	Vijaya	Phani	Updated logo and information classification	Modified as per new document and updated new information classification
7.00	30-Dec-20	Divya	Vijaya	Phani	Periodic Review & Update	Approved and Baselined

7.1	3-Jan-2022	Divya	Vijaya		For Review	Modified as per the new template
8.00	13-Jan-2022	Divya	Siva N	Siva N	For Approval	Approved and Baselined
8.1	14-Mar-22	Sanjana	Divya	Siva N	For Review	The scope has been extended to products and services
9.0	18-Mar-2022	Sanjana	Divya	Siva N	For Approval	Approved and baselined
9.1	10-Mar-2023	Beniyel S, Pallavi Chakrabarty	Balu N			New template change
10.0	12-May-2023	Beniyel S	Balu N	Srikanth M	For Approval	Approved and Baselined
10.1	23-Jan-2024	Rakesh Vijendra			For Review	Requirement from ISO27001:2022 of Secure Coding & Secure system architecture & engineering principle has been addressed
11.0	23-Feb-24	Vijaya	Vijaya and Bala	Srikanth	For Approval	Approved and Baselined

11.1	6-May-25	Balu Nair	Vijaya		Yearly Review	Migrated to a new Template
12.0	14-May-25	Balu Naifr	Vijaya	Srikanth M	For Approval	Approved and Baselined

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com