TRIANZ℠

SECURE SYSTEM ARCHITECTURE AND ENGINEERING PRINCIPLES

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. Objectives

The objective of this procedure is to provide the guidelines on secure system architecture and engineering principles that are established in the organization.

2. Scope

This procedure is applicable to all new and existing systems and application architecture developed at Trianz.

The procedure applies to all managed Trianz products and services.

3. Security Principles

- Security Foundation
- Risk Based
- Ease of Use
- Increase Flexibility
- Reduce Vulnerabilities
- Security by design
- Defense in depth
- Security by default
- Fail Securely
- Never trust inputs from external sources or applications
- Secure deployment
- Always assume breach - design or implement controls accordingly.
- Always follow least privilege or default deny rules.
- Always design usability and manageability and least functionality in mind.

4. Security Foundation

The principles related to Security foundation are specified below

- To establish a sound security policy as the "foundation", the Information Security Policy is defined and implemented. The policy identifies security objectives like
- To ensure confidentiality, integrity and availability of critical information at all times
- To protect information assets
- To protect critical information from unauthorized access, use, disclosure, modification, and disposal, whether intentional or unintentional
- To Implement security requirements from the initial level of the project initiation
- Understanding the security requirements
- Implementation of security requirements such as
- User authentication
- Secure session controls
- LDAP authentication
- Role based security implemented
- Rule or Role or attribute based access control with least privilege or default deny policy.
- Tracking the user activities while changing the data
- Data is encrypted at database level to avoid the access to other users
- User activities are tracking while read access at database level. (Query band implementation)
- Participating in the evaluation of security products
- Define physical and logical security boundaries
- Physical Access – Access control mechanism is implemented
- Logical access at application or product level is provided based on the requirements
- Ensure that project team to develop and validate secure application
- Define security standards like encryption algorithms to be used, etc as per the project requirements
- Train the team on the defined standards
- Periodically perform Threat Modeling on the applications and cover all the known threats, attack patterns and vulnerabilities as per Threat Modeling procedure.

- Security shall be designed and integrated at all architecture layers (DB, network, application, platform etc.)
- Implement DLP and Dynamic access management wherever required.
- Always follow secure design principles and perform security-oriented design reviews.
- Follow system hardening procedures and perform TVM regularly.
- Trianz shall design or architecture information systems by following zero-trust principles in mind.
- Wherever possible use immutable infrastructure.

5. Risk Based

- Perform Risk Assessment, the risk treatment should ensure the risk handling for reducing the risk to acceptable level which is applicable for all projects
- Based on the risk assessment, all the required controls like encryption, integrity checks, digital signatures, data validation, tokenization, anonymization, Pseudonymization need to be implemented.
- Implement control that can detect, prevent and respond to security events, incidents, attacks.

6. Secure Development

- Secure Development shall adopt "Microsoft Secure Development guidelines" or an equivalent methodology of Secure Software Development Life Cycle.

7. Secure Implementation

- Multilayer access approach implementation can protect an asset from unauthorized access or modification

- By Implementing layered security, the project team will protect application layer, Database layer, Integration layer and Data
- Application layer will be protected like LDAP authentication, Credentials
- Technical review compliance will be verified by Delivery Assurance in check points and toll gates

8. Ease of Use

- Where possible, base security on open standards for portability and interoperability will be implemented
- Use common language in developing security requirements
- Design security to allow for regular adoption of new technology, new platforms and including a secure and logical technology upgrade process

9. Reduce Vulnerabilities

- Identify and prevent common errors and vulnerabilities, such as buffer overflows, race conditions, format string errors, failing to check input for validity, and programs being given excessive privileges.
- Implement profile or role privileges which will reduce risk by limiting the number of people with access to critical system security controls
- Implementing role-based access controls for various aspects
- Controlling who is allowed to enable or disable system security features or change the privileges of users or programs
- Application vulnerabilities like crosstie scripting, SQL injection and etc. can be reduced by following the coding standards like prepared statements in Java and during testing also can be identified by the browser plug-ins like tamper IE
- SSL implementation for secure transactions, by installing SSL certificates

10. Reference(s)

- From implementation guidelines of ISO 27002:2022 and CSA star guidelines.

11. ISO Control Mapping

Category of Control	**ISO 27001:2022 Control**	**Document Name as per ISO 27001:2022**
8.27 Preventive	Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities.	#Application_security #System Architecture

Document Control

Owner:	CISO	**Release ID:**	SEP-GUID-0066

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.1	4-May-15	Sudharsana	Balu Nair		Initial draft	None
1.0	15-May-15	Srilakshmi	Balu Nair	Zulfikar Deen	Baseline is approved by Zulfikar Deen.	Approved Baseline.
1.1	25-Jan-16	Paramita Ghosh and Balu Nair	Vijaya	Zulfikar Deen	Adding security foundations points	Adding security foundations
2.0	08-Feb-16	Balu Nair	Vijaya	Updated references section	Approval for Baseline	Baselined references section
2.1	09-Feb-24	Sraveen	Balu	Srikanth Mantena	For review	Added CSA star in the reference section Added security architecture principles.

						Modified in alignment to ISO 27001:2022
3.0	23-Feb-24	Sraveen	Vijaya	Srikanth Mantena	For Approval	Approved and Baselined
3.1	28-May-25	Kruti	Vijaya		For Review	Migrated to New Template
4.0	29-May-25	Kruti	Vijaya	Srikanth Mantena	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com