TRIANZ℠

# Application Security 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 that all applications must implement adequate security measures to protect the Confidentiality, Integrity, and Availability of data at rest, in use or in motion.
- The application security policy defines the security framework and requirements for applications, notably API & web applications, within Trianz's production environment.

## 2. Objective

- The objective of this policy is to provide guidance and support to project, products and development teams in delivering secure applications to support the Trianz's business while expediting the security assessment and testing process required to validate new application releases ensuring they are free of vulnerabilities that would put the production environment at risk.

## 3. Scope

- All applications that pass or store data owned by Trianz are subject to this policy. This policy applies to all applications within Trianz's production environment, as well as administrators and users of these applications.
- All externally accessible public facing applications, internally accessible mission critical applications, and vendor customizable Commercial Off-The-Shelf (COTS) or in-house developed applications and cloud-based applications are included within the scope of this document.
- The policy is applicable for all Trianz products and services.

## 4. Policy Statements

Secure development practices will be established, implemented, and documented for all applications developed or purchased to include appropriate security controls to prevent unauthorized access or modification of the system or information coded or stored.

## 4.1 Application Security Metrics

Technical and operational metrics shall be implemented according to business objectives and security requirements.
Refer to Trianz Metrics Strategy document.

## 4.2 Data Security

Protecting data's confidentiality, integrity, availability and privacy. Privacy is a principle that must be maintained at all times. Proper encryption solutions must be implemented to protect data at rest, in use or in motion.

## 4.3 Access Control

All access to Trianz's systems must be authorized and based on individual identification and authentication. Application logs are to be designed to showcase application user activity audit trails.

## 4.4 Infrastructure Security

- Application hosting solutions must comply with the Trianz's security policies and standards and have a Service Level Agreement defined with the infrastructure provider.
- The infrastructure environment, IAAC, Container images must be scanned on a periodic basis to identify security vulnerabilities, misconfiguration or missing security patches. (Vulnerability Management Policy).
- For cloud or Software as a Service solutions (SaaS) third party vendors must provide evidence that periodic security scans, assessments or audits are conducted on their infrastructure environment and findings are addressed in a timely manner.

## 4.5 Application Environment

- Infrastructure environments hosting application binaries or source code must have security mechanisms in place to prevent unauthorized access and modification of resources or data.
- Change control procedures must be defined to ensure that only authorized changes after passing through the required phase gates, approved by the business and reviewed by the Trianz's Information

Security & Data Privacy Assurance team, can be released in a production environment. (C.f. Change Management Policy). Deviation in the phase gates would need approval from internal & external stakeholders. Development & testing activities should not be conducted in production environment. No production data can be used for trouble shooting in non-production environment. Engineering team members should not be provided access to the production environment. If there's specific production access required for trouble shooting, same is to be provided temporarily with required deviation approval.

- Separation of duties must be implemented to protect the production environment from unauthorized access or modification.
- A risk assessment shall be performed prior to production for all applications that will store, access, create, and/or transmit confidential or protected information.

## 4.6 Security Assessment and Releases to Production

- All modifications of the application must go through a change release process that includes an appropriate security assessment (automated security scanning or manual testing) to identify potential risk and security impacts to the current production environment.
- Any application change being deployed in a production environment must ensure compliance with the Trianz's security policies, standards, and best practices. Successful completion of the security assessment is acknowledged by the Trianz's CIO or CISO, and must be achieved prior to launch in production.
- Each release must have a defined roll-back plan in case its migration to the production environment causes service degradation.

### 4.6.1 Security Assessment Level

The following security assessment levels are established.

- Full assessments test for all known web application vulnerabilities using both automated and manual tools. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities and determine the overall risk of those vulnerabilities.

- Quick assessments will at a minimum consist of an automated scan for the OWASP Top Ten web application security risks.

### 4.6.2 Releases to production

- Releases to a production environment are approved based on the vulnerabilities found during the security assessment.
- All security issues that are discovered during assessments or identified by the Trianz's Software Security Assurance Tool must be mitigated based upon the following risk levels, which are based on the Open Web Application Security Project (OWASP).
- Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of medium risk level or greater.

## 4.7 Business Continuity

- Application business owners must ensure that each application has a defined Business Continuity Plan and a Disaster Recovery Plan to ensure its readiness to respond to events that could disrupt the application's service continuity.
- Back-up & recovery plans and solutions shall be designed according to business requirements.
- For services provided by Third Party vendors, business owners must define the provider's Service Level Agreement (SLA) with these requirements taken into consideration.

## 4.8 Application End of Life

- Decommissioning an application requires the same security precautions as maintaining it in production.
- Regulatory requirements about data retention and destruction must be considered as application is decommissioned.
- If an application cannot maintain compliance with the Trianz's policies and standards.
- Trianz's CIO/CISO may provide binding recommendations to mitigate outstanding risks.

## 2. Applicable standards

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

## 3. Reference Policies & Procedures

- Information classification policy
- Access Control policy
- Business Continuity
- Change Management Policy

## 4. 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.

## 5. ISO Control Mapping(s)

| **Category of Control** | **ISO 27001:2022 Control** | **Document Name as per ISO 27001:2022** |
|---|---|---|
| Technological Controls | 8.26 Application security requirements-<br>Control Information security requirements shall be identified, specified and approved when developing or acquiring applications. | Application Security Policy |
| Technological Controls | 8.18 Use of privileged utility programs | |

## Document Control

| **Owner:** | CISO | **Release ID:** | APS-POL-0043 |
|---|---|---|---|

**For Trianz Process Improvement Group (TPIG) Purpose Only**

### Version History

| Ver. No. | Date | Author | Reviewer | Approver | Reason for Change | Change Description |
|---|---|---|---|---|---|---|
| 0.1 | 21-May-18 | Kamadeva Pradhan | Joshy VM, Balu Nair, Gangadhar Aka,Vishwanath MS, Himayat | | Initial | Initial Draft |
| 1.00 | 23-Jun-18 | Kamadeva Pradhan | | Ganesh Arunachala | Approved by Ganesh | Baselined |
| 1.01 | 29-Apr-19 | Balu Nair | Joshy VM | | | Information classification modified |
| 2.0 | 14-May-19 | Balu Nair | | Ganesh Arunachala | Approved for Release | Baselined |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | la | | |
| 2.1 | 11-May-20 | Karthik N | Balu Nair | | Review | Roles modified with CIO/CISO and Formatting changes |
| 3.0 | 14-May-20 | Karthik N | Phani Krishna | Phani Krishna | For Approval | Approved and Baselined |
| 3.1 | 23-Jan-21 | Divya G | Phani Krishna | Phani Krishna | For Review | Updated with new information classification |
| 4.0 | 23-Jan-21 | Divya G | Phani Krishna | Phani Krishna | For Approval | Approved and Baselined |
| 4.1 | 08-Nov-21 | Divya G | Phani Krishna | Phani Krishna | For Review | Modified as per new template |
| 5.0 | 08-Nov-21 | Divya G | Phani Krishna | Phani Krishna | For Approval | Approved and Baselined |
| 5.0 | 06-Jan-2022 | Divya | Karthik | Siva N | For review | Reviewed and no changes |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | in the document |
| 5.1 | 23-Feb-22 | Sanjana | Karthik | | For review | The scope has been extended to products and services |
| 6.0 | 22-Mar-22 | Sanjana | Siva N | Siva N | For Approval | Approved and baselined |
| 6.1 | 26-April-23 | Krutideepta, Pallavi Chakrabarty | Vijaya R | Srikanth M | For Review | Migrated to new template |
| 7.0 | 12-May-23 | Krutideepta | Vijaya R | Srikanth M | For Approval | Approved and baselined |
| 7.1 | 15-Feb-24 | Shalini | Vijaya | | For Review | Mapped with New ISO 27001, 2022 control 8.26 |
| 8.0 | 23-Feb-24 | Shalini | Vijaya | Srikanth | For Approval | Approved and baselined |

| | | | | | | |
|---|---|---|---|---|---|---|
| 8.1 | 15-Apr-2025 | Vijaya | Balu | | For Review | Migrated to a new template and Yearly Review |
| 9.0 | 14-May-2025 | Vijaya | Balu | Srikanth | For Approval | Approved and baselined |

## Contact Information

Name

Email

Phone

# Thank You

Infosec@trianz.com