TRIANZ℠

# Supplier 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

This document specifies the requirements that must be met by suppliers in handling, management, storage and processing of information belonging to Trianz and Trianz clients.

## 2. Scope

This policy is applicable to all third party, contract suppliers including cloud service providers and vendors offering products and services to Trianz and its clients.

## 3. Policy Statements

Trianz Information security requirements for mitigating the risks associated with supplier's access to the organization's assets are agreed with the supplier and documented.

Trianz must identify and mandate information security controls to be addressed by supplier, such as:

- Identify and document the types of suppliers including cloud service providers.
- Rank the supplier based on the confidential & personal data being exchanged and also the financial value.
- Respective functional coordinators from projects and functions shall perform vendor risk assessment for their critical vendors.
- Information security and privacy risk assessment of all critical vendors shall be conducted at least annually by respective functional coordinators.
- Once the risk assessment form is obtained by the vendor, information security team shall review and provide feedback to the respective functional coordinator.
- Respective functional coordinator shall coordinate with the vendor to close the review feedback.

- Define the types of access that are allowed to suppliers. – incomplete
- Minimum information access (least privilege) to the supplier.
- Types of obligations to supplier to protect organization information.
- Handling of incidents associated with suppliers.
- Business continuity for the information provided by either parties.
- Security requirements and controls documented in agreement signed by both parties.

## 3.1 Information security policy for supplier relationships

- Information security requirements should be addressed to secure the processes and procedures to ensure appropriate controls that may be implemented either within the organization or by the suppliers, cloud service providers and cloud service customers.
- Access control, especially for sensitive information must be accurately defined, managed and monitored.
- Awareness training for both the organization's staff and supplier staff that handle or interact with sensitive data shall be addressed.
- Service transitions should be documented and include procedures for secure data transfers and availability as the supplier relationship changes during the course of time.

## 3.2 Addressing security within supplier agreements

All relevant information security requirements are established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the Trianz data.

Supplier agreements should be established and documented to ensure there is no misunderstanding regarding both parties' obligations to fulfill relevant security requirements. Supplier agreements should include clear and concise information regarding:

- Trianz data classification requirements as it apply to the supplier.
- Definition of acceptable uses for the data handled by the supplier.
- Processes and procedures for monitoring compliance with the contract requirements.
- A "right to audit" the supplier or regular access to external assessments, as applicable  Conflict and defect resolution.
- Required screening, training or other obligations of the supplier's staff.
- The use of sub-contractors to provide services and the extension of security requirements to them. It is important to address the risk early in the procurement phase of the relationships with external parties so that roles, and responsibilities and expectations can be clearly defined in agreements or contracts.
- Ensure Security patch compliance by the Suppliers / vendors and also ensuring the verification to the Vendor Risk Assessment/ Periodic vendor audits.

As a cloud service customer, information security roles and responsibilities shall be defined related to the cloud services as below,

- Malware protection
- Backup
- Cryptographic controls
- Vulnerability management

- Incident management
- Security testing and auditing etc.
- Authentication and access control

As a cloud service provider, necessary information security measures need to be taken and ensured that there is no disagreement between cloud service provider and customer.

### 3.3 Information and communication technology supply chain

- Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.
- Trianz information and communication technology supply chain is specifically related to their use of technology, both software and hardware. – a statement not a command
- There shall be a process to identify a product or service that is critical, and requires increased scrutiny.
- Trianz shall address the risks of a component or service becoming unavailable or no longer supported.
- Trianz shall perform risk assessment of information processing and storage vendors/suppliers at the time of their termination or service no longer required.

## 4. Exceptions(s)

There is no exception to this policy.

## 5. ISO Control Mapping(s)

| Category of Control | ISO 27001:2022 Control | Document Name as per ISO 27001:2022 |
|---|---|---|
| Organizational controls | 5.19 Inform action security in supplier relationships Control Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services. | Supplier Security Policy |
| Organizational controls | 5.20 Addressing information security within supplier agreements within supplier agreements Control Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship. | Supplier Security Policy |
| Organizational controls | 5.21 Managing information security in the information and communication technology (JCT) supply chain Control Processes and procedures shall be associated defined and with implemented the ICT products to manage and the information security risks services supply chain. | Supplier Security Policy |
| Organizational controls | 5.22 Monitoring, review and change management of supplier services Control The organization shall regularly monitor, review, evaluate and | Supplier Security Policy |

| | | |
|---|---|---|
| | manage change in supplier information security practices and service delivery. | |

# Document Control

| **Owner:** | CISO | **Release ID:** | SSP-POL-0029 |
|---|---|---|---|

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

### Version History

| Ver. No. | Date | Author | Reviewer | Approver | Reason for Change | Change Description |
|---|---|---|---|---|---|---|
| 0.01 | 28-April-15 | Sudharsana.cv | | | Initial Draft | None |
| 1.00 | 19-May-15 | Sudharsana.cv | | | Reviewed by CISO | Approved |
| 1.01 | 14-Oct-16 | Sriharsha | | | Addition of Cloud services as scope of Certification. | Scope section is modified<br>Modified Trianz Logo |
| 2.00 | 07-Dec-16 | Balu Nair | | | Approved by CISO | Baselined |

| | | | | | | |
|---|---|---|---|---|---|---|
| 2.1 | 07-Nov-19 | Karthik N and Balu Nair | Phani Krishna | | Review | Added cloud aspects of supplier security |
| 3.0 | 22-Nov-19 | Karthik N | | Vivek Sambasivam | Approved for Release to Blue Book | Baselined |
| 3.1 | 13-May-20 | Balu Nair | Phani Krishna | | | Migrated to the new template |
| 4.0 | 14-May-20 | Balu Nair | Phani Krishna | Phani Krishna | For Approval | Approved and Baselined |
| 4.1 | 18-Jan-21 | Karthik N | Phani Krishna | | For Review | Updated the information classification and format level changes |
| 5.0 | 18-Jan-21 | Karthik N | Phani Krishna | Phani Krishna | For Approval | Approved and Baselined |
| 5.1 | 3-Jan-22 | Divya G | Karthik N | Sivaramakrishnan N | For Review | Modified as per the new template |
| 6.0 | 13-Jan-2022 | Divya G | Karthik N | Sivaramakrishnan N | For Approval | Approved and Baselined |

| | | | | | | |
|---|---|---|---|---|---|---|
| 6.1 | 15-07-2022 | Divya G | Karthik N | | For review | Modified the policy statements. |
| 7.0 | 15-07-2022 | Divya G | Karthik N | Sivaramakrishnan N | For Approval | Approved and baselined |
| 7.1 | 10-Mar-2023 | Beniyel S, Pallavi Chakrabarty | Balu N | | For review | New template change |
| 8.0 | 12-May-2023 | Beniyel S | Balu N | Srikanth M | For Approval | Approved and Baselined |
| 8.1 | 11-Feb-2024 | Beniyel S | Vijaya R | Srikanth M | For Review | ISO Control Mappings Has been added. |
| 9.0 | 23-Feb-2024 | Beniyel S | Vijaya R | Srikanth M | For Approval | Approved and Baselined |
| 9.1 | 30-Apr-25 | Kruti | Vijaya R | | For Annual Review | Migrated to a new Template and Yearly Review |
| 10.0 | 14-May-25 | Kruti | Vijaya R | Srikanth M | For Approval | Approved and Baselined |

TRIANZ℠

## Contact Information

Name

Email

Phone

# Thank You

infosec@trianz.com