TRIANZ℠

SHARED SECURITY RESPONSIBIILTY MODEL 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 provide security and compliance responsibilities shared between the Service Provider and the Customer when hosted in the Cloud along with the supply chain partner's management.

2. Objectives

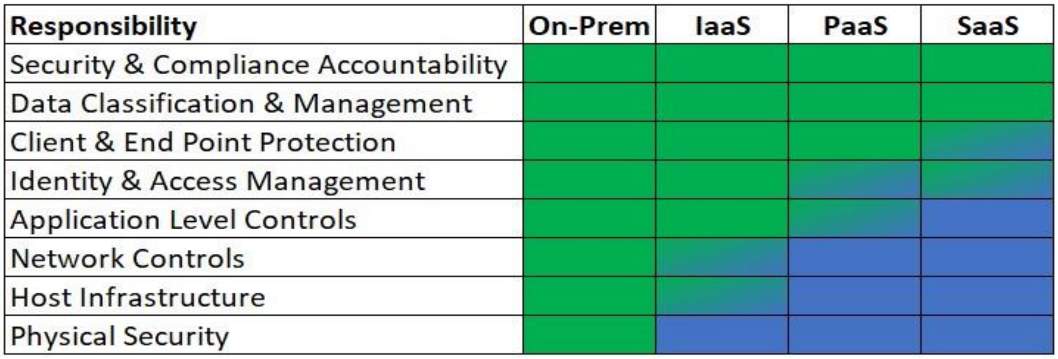
The objective of Shared Security Responsibility Model Policy is to facilitate effective implementation of the security & controls for the different controls for the available cloud service models.

3. Scope

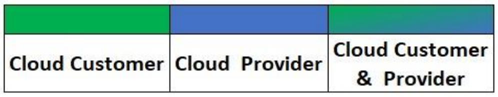
This policy document covers the Shared Security Responsibility Model in the Cloud where Trianz act as an CSC or CSP for the different Managed Cloud Service Models.

4. Policy Statement

4.1 Cloud Shared Responsibilities – Provider vs Customer:



Responsibility	On-Prem	IaaS	PaaS	SaaS
Security & Compliance Accountability	🟩	🟩	🟩	🟩
Data Classification & Management	🟩	🟩	🟩	🟩
Client & End Point Protection	🟩	🟩	🟩	🟩🟦
Identity & Access Management	🟩	🟩	🟩🟦	🟩🟦
Application Level Controls	🟩	🟩	🟩🟦	🟦
Network Controls	🟩	🟩🟦	🟦	🟦
Host Infrastructure	🟩	🟩🟦	🟦	🟦
Physical Security	🟩	🟦	🟦	🟦



🟩	🟦	🟩🟦
Cloud Customer	Cloud Provider	Cloud Customer & Provider

- ***Basic Definitions:***

  On-Prem – Customer may have a hybrid cloud environment where some of the equipment are managed on-prem. All the responsibilities of the On-prem infrastructure are to be owned and handled by the Customer

IaaS – Infrastructure as a Service provides infrastructure (servers and networking devices/services) and allows customers to install software, provision virtual servers, containers and control the configuration of all mentioned

***PaaS* –** Platform as a Service provides computing platform and technical stack as a service. Customers focus the energy only on build and manage application. Example: AWS Lambda

***SaaS* –** Software as a Service provides entire infrastructure and the application. Customer only logs in and uses the Application provided by the Provider

Identity - Enables the user to define who is with a user id, employee number etc.,

Authentication - Verifies who the user is based on the enabled credentials

Authorization - Determines what a user can and cannot access

Accountability - Ensures enabling non-repudiation i.e., ensuring the actions performed by the user is traceable to make him/her accountable

Customer content - Includes but not limited to data, text, image, audio, video, customer developed software, customer configured machine images, customer code including infrastructure codes.   Customer Account information managed by the Provider is not classified as Customer Content

4.2 Responsibility:

4.2.1 Security & Compliance Accountability:

- The responsibilities of security and compliance may be delegated but the Customer is ultimately accountable for the Security & Compliance irrespective of the Cloud Service Model
- Customer should ascertain all the Shared security responsibilities throughout the supply chain including the service provider are documented, implemented, and managed

- The Customer is ultimately accountable for the security and compliance of the platform

4.2.2 Data Classification & Management:

- Customer is responsible for data is securely identified, labeled, and correctly classified to meet any compliance obligation in all the Cloud Service Models
- Providers should provide written contracts on how the customer data security & privacy will be managed in the Cloud
- The Provider's written commitments should state Provider's security & privacy practices, limitations of the Customer data use, and the regulatory compliance adhered, to showcase evidence of the certifications and audit reports on demand by the customer
- Customer should ascertain that the cloud provider is consistent with the above controls periodically and should move away if the cloud provider cannot address the data protection needs
- ***IaaS Service Model –*** Provider capabilities are limited to enable Customer's virtual environment can accommodate the data classification capabilities. Customer's responsibility is to configure and protect the data that is stored and configured. Customer should ascertain data classification is enabled at all layers of the solution.
- ***PaaS Service Model –*** Provider capabilities are limited to enable Customer's virtual environment & application can accommodate the data classification capabilities required for the Customer. PaaS providers responsibility will be limited with authentication and the Customers would need to configure and handle authorization for the user's data access
- ***SaaS Service Model –*** Provider would need to enable for data protection, user authentication and user authorization. Customer would be responsible for configuring the data authorization for the user based on the defined roles.

4.2.3 Client & End-point protection:

- Provider will be responsible for enabling the end-point protection of the cloud services rendered to its customer on all cloud service models
- Customer will be responsible for ascertaining security of the devices that are used to connect to the cloud services
-

- Customer to ascertain all the cloud connecting endpoint devices are hardened, patched, encrypted, and secured with mobile management solutions which provide remote wipe like services during a theft scenario
- Provider would need to provide services which will facilitate the Mobile management capabilities at the customer end-point devices and to be configured suitably by the Customer in SaaS Model.

4.2.4 Identity & Access Management:

- Identity & Access management enables implementation of IAAA – Identity,
- Authentication, Authorization & Accountability security principles on the cloud platform.
- **IaaS Service Model –** Provider delivers capabilities for IAM solutions and Customers must configure and manage the Identity & Access management controls
- **PaaS & SaaS Service Model –** IAM Controls are shared responsibility between Customer and Provider for these service models. The identity provider, identity services configuration, user roles, user identities configuration, access control configuration to be considered and implemented for an effective solution
- Additional security considerations viz., Just in Time (JIT) administrative access, MultiFactor authentication, role based access control (RBAC) capabilities availability(Own or third-party applications) and effectiveness with the provider are to be assessed by the Customer before implementation

4.2.5 Application-Level Controls:

- The application-level controls are to secure the application layer from any security breaches
- ***IaaS Service Model –*** Customer will be responsible for protecting the application layer deployed on the Virtual machines/Containers to protect the application from any attacks, breach, or compromises. Customer would need to deploy skilled administrators who will be able to manage and secure the application and underlying hosts
- ***PaaS Service Model –*** PaaS Service model application controls are shared responsibility between Customer & Provider. Provider will deliver application

controls with default configurations and the Customer would need to configure suitably for the security/business needs.

- ***SaaS Service Model –*** Application layer security controls are the Provider responsibility and Provider's compliance; audit reports can be used by Customer for evidencing the application layer controls

4.2.6 Network Control:

- Network control enables securing and configuring the inter/intra connectivity of the platform
- The network of the elements to be secured includes but not limited to Virtual Machines, Containers, Pods, Virtual networks, perimeter devices, gateways, Proxies, load balancers, DNS solutions etc.,
- ***IaaS Service Model –*** Provider would be responsible for the network security of the underlying infrastructure provided by the provider across regions, availability zones etc., Customer will be responsible for the network security of the devices and services he deployed in the infrastructure instances managed by him
- ***PaaS & SaaS Service Model –*** Network Security control is abstracted from the customers and provided as part of the service by the Provider. Provider holds responsibility of the network security control.

4.2.7 Host Infrastructure:

- The host infrastructure security controls include protecting, managing & securing the compute, storage & platform services.
- Different controls for host infrastructure are OS configuration, hardening, Patching, Access control management and identity control configurations.
- ***IaaS Service Model –*** Host infrastructure security is a shared responsibility between the Customer and the Provider. Providers will ascertain the host security is deployed on the underlying hardware for the VMs hosted for the Customers. Providers take responsibility of the VM freeze in case of any reboot required for the patches and adheres to the SLA promised to the Customer.   Customer will be responsible for enabling all the host infrastructure security controls in their instances.
- ***PaaS & SaaS Service Model –*** Host infrastructure security control is abstracted from the customers and owned by the provider.

4.2.8 Physical Security:

- Buildings, facilities where the servers, storage and network equipment are physically hosted to provide cloud services are to be considered for the physical security.
- Providers are responsible for defining the policies, procedures and processes for the physical security of the infrastructure.
- Providers should provide promised uptime by designing/deploying high availability for Power, HVAC, network connectivity
- Providers to enable the disaster and recovery management for the physical environment
- Customer to exercise rights as part of the agreement with provider to obtain audit and compliance certification. These certificates can be presented as compliance evidence for Customer's audit standards
- If the compromised key is KEK or a master key from which other keys are derived, then all keys hierarchically under it must also be revoked and replaced
- If the compromised key is a working key, then data associated with such key must be revoked and re-encrypted with new working key in accordance with the policy
- There must be investigation triggered including Infosec team on any key compromise followed by root-cause and remediations detailed

4.3 Provider Responsibility:

- All customer content is to be stored only in the geographic location chosen and provider should not move without explicit permission from the Customer
- Customer should be enabled by the provider to download, delete transfer their data out of the Provider infrastructure based on customer need
- Customer should be enabled by the provider to encrypt the content with their own keys
- Provider to provision enabling crypto-delete for customer to delete their content and Customer encryption keys

- Provider to enable customers for using many security techniques such as encryption, tokenization to protect the content

Agreements between the provider and the customer to clearly state the approvals for sharing data for complying to law, binding orders from Government and regulatory bodies

- Provider should give details about the request reports from law enforcement, government, regulatory body binding regularly to its customers
- Provider to implement the finalized SSRM with the Customer. Need to document & test the operation of security control implementations which must include the interdependencies/integration validation.
- Provider should manage, monitor & audit the service performance as per agreed SSRM with the Customer.
- Provider should maintain inventory of all the supplier partners in the supply chain and maintain transparency with the customers on the list
- Provider should ascertain the following are stated in the service agreements with the Customers:
- Scope, characteristics, and location of business relationship and services offered
- Information Security requirements expected from the Customers (including SSRM)
- Change management process
- Logging & monitoring capabilities
- Incident management & communication procedures
- Right to audit & third-party assessment available for the customers
- Clauses related to service termination
- Requirements for interoperability and portability
- Data privacy
- Provider should list and ascertain all the policies required for maintaining the CIA & P of

Provider & Customers are available with the supply chain partners. Minimum Service Level requirements not exceeding Client SLAs are to be signed with the Supply chain partners

- Provider should ascertain all the supply chain partners risk factors, IT Governance policies & procedures are periodically evaluated & updated
- Provider should all ascertain any security certification standards (Ex: ISO 27001, PCI

DSS) required for the Customers are available and active with the supply chain partners

- Provider should ascertain all the supply chain partners are security assessed periodically (Minimum of one assessment per year)

4.4 Customer Responsibility:

- Customer to state and include the following in the provider and other supply chain organization agreements:
    - Right to audit
    - Service termination clause
    - Third party security assessments
    - Interoperability & portability requirements
    - Data privacy requirements
- To periodically review the supply chain partners including Provider Governance policies and procedures
- To periodically conduct security assessments of all organizations including the provider servicing the customer

  To review the agreements with the supply chain organizations including the provider at least annually
- To maintain an inventory of the supply chain organizations and the services rendered.

5. Roles & Responsibilities

Roles	Responsibilities	Internal/External
Project/Platform/Product Security, Cloud, infra management team	Adhere to the SSRM policy based on the Customer/Provider role for the engagement	Internal
Product Owner /Project Manager/Operations Manager	Validate the SSRM controls are implemented as the policy	Internal

InfoSec & Compliance Team	Validate the SSRM Process & responsibilities are adhered as per the policy	Internal

6. Applicable Standards

- NIST.SP.500-322
- NIST.SP.500-292
- PCI DSS Cloud Computing Guidelines

7. Exception(s)

There is no exception to this policy

8. Annexure – CSP & CSC Responsibilities Template

Responsibility/Area	Tools	CSP Control	CSC Control
IAM	KeyCloack	Yes	
Encryption at rest	Hashicorp	No	Yes
Encryption at rest	KMS	Yes	Yes
		Shared	Shared

9. ISO Control Mapping

Category of Control	**ISO 27001:2022 Control**	**Document Name as per ISO 27001:2022**
Technological Controls	5.23 Information security for use of cloud services Control Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.	Shared Security Responsibility Model Policy

Document Control

Owner:	CISO	Release ID:	SSRM-POL-01

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.1	20th Jun 22	Divya	Balu Nair	Siva N	Initial Version	None
0.2	18th Jul 22	Divya	Balu Nair	Siva N	Amendments post internal review	To include specific inputs on Transparency & Accountability
1.0	11th Aug 22	Divya	Balu Nair	Siva N	Baselined	Approved and Baselined
1.1	26-April-2023	Krutideepta, Rama Madhavan	Vijaya R	Srikanth M	For Review	Reviewed with no changes Migrated to new template
2.0	12-May-2023	Rama Madhavan	Vijaya	Srikanth M	For Approval	Approved and Baselined
2.1	15-Feb-23	Shalini	Vijaya	Srikanth	For Review	Mapped with new ISO control 5.23

3.0	23-Feb-23	Shalini	Vijaya	Srikanth	For Approval	Approved and Baselined
3.0	24-Feb-24	Shalini	Vijaya	Srikanth M	For Review	Reviewed with no changes
3.1	28-May-25	Kruti	Vijaya		For Review	Migrated to new template.
4.0	29-May-25	Kruti	Vijaya	Srikanth M	For Review	Reviewed with no changes

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com