



Cloud 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

<input type="checkbox"/>	Public
<input checked="" type="checkbox"/>	Internal
<input type="checkbox"/>	Confidential
<input type="checkbox"/>	Restricted

Table of Contents

1. PURPOSE	5
1.PURPOSE	ERROR! BOOKMARK NOT DEFINED.
2. POLICY	5
2.1 ASSET MANAGEMENT	6
2.2 MULTI-TENANT ENVIRONMENT AND CLIENT DATA ISOLATION	6
2.3 ENCRYPTION	7
2.4 IDENTITY, ACCESS AND PRIVILEGE LOGIN MANAGEMENT	7
2.5 INCIDENT MANAGEMENT	8
2.6 GEOGRAPHIC LOCATION FOR SETTING UP CLOUD	8
2.7 SUPERVISORY AUTHORITIES	9
2.8 COMPLIANCE REQUIREMENTS	9
2.9 VULNERABILITY MANAGEMENT	9
2.10 SECURE DISPOSAL	10
2.11 LOGGING AND MONITORING SECURITY INCIDENTS	10
2.12 LICENSING REQUIREMENTS	11
2.13 HARDENING	12
2.14 FOLLOWING MUST BE ADHERED TO PASSWORD MANAGEMENT FOR PRIVILEGED AND NON-PRIVILEGED PASSWORDS.	12
2.15 VIRTUALIZATION	12
2.16 INFORMATION BACK UP	14
2.17 CHANGE MANAGEMENT	15
2.18 CLOUD SERVICE PROVIDER MANAGEMENT	15
2.19 ROLES AND RESPONSIBILITIES	16
3. EXCEPTIONS(s)	18

1. Purpose

The purpose of this document is to provide directions on Trianz Policies for ensuring security and Privacy of information in the Cloud environment, in the below scenarios:

- Cloud based service provided to Client where Trianz acts as a Cloud Service Provider
- Cloud based service consumed by Trianz where Trianz acts as a Cloud Service Customer
- As a cloud-based Service Provider, all the below Policies must be implemented by default in the absence of any specific Client requirements
- As a cloud Service customer all the below Policies implementation must be ensured.

The Services offered or consumed either in the role of a Cloud Service Customer or a Cloud Service Provider can vary from "Infrastructure As a Service (IAAS), Platform As a Service(PAAS), Software As a Service (SAAS) or simply Device Managed Services.

This policy has to be read along with Trianz **Information Security Policy** and **Data Protection and Privacy Policy** as applicable from time to time.

2. Policy

All the below policies will be applicable to all scenarios where Cloud based environments are involved unless there are specific Client contractual requirements which must be met, wherever applicable.

2.1 Asset Management

- All Cloud related assets must be identified as part of Asset Inventory. This includes but not limited to all virtual assets, active and inactive images, hypervisors,
(applicable if Cloud Service Provider, Cloud Service Customer/User)
- The records of the inventory must indicate where the assets are maintained, location and details of cloud also and shall be reviewed periodically (applicable if Cloud Service Provider, Cloud Service Customer/User)
- For all Cloud services that are offered, identify Cloud service data and Cloud service derived data (shared responsibility of Provider and Customer)
- Project Managers shall be responsible for Cloud assets Management (safeguarding the assets) during the Project Execution. In addition, the responsibility of client provided assets shall be as per contractual agreement.
- All Cloud assets shall be labelled to ensure identifying the resource utilization.
- Asset inventory shall be maintained and risk management shall be conducted using EMPMO tool/ PMWork book by respective PMs(including Subscriptions)

Please refer to **Asset Management Policy** for other details.

2.2 Multi-Tenant environment and Client Data Isolation

- In multitenant environments, segmentation between resources and those of other clients, as well as between own instances must be assessed in line with Trianz Information Security and Cloud Security Policies.

- Leverage a zone approach to isolate instances, containers, applications, and full systems from each other when feasible.
- Must implement filtering on incoming and outgoing traffic, wherever feasible. 1. Must implement technical controls to limit the access for downloading of data from the cloud environment to end user systems i.e. access limited to only for the authenticated resources ,. This can be implemented by deploying terminal servers and allowing authorized user to login to this server and connecting to cloud systems. This requirement must be analyzed based on the client's and / or regulatory requirements For all internal applications & Cloud Services, Single Sign on shall be enabled

2.3 Encryption

- All confidential data including Personal and Sensitive Data at rest and in transit shall be encrypted on Cloud
- All Backup files stored on Cloud must be volume level encrypted.
- For all Client managed data, encryption shall be as per Contractual agreement and as per the laws of the land.

Please refer to **Encryption Policy** for more details.

2.4 Identity, Access and Privilege Login Management

- Enforce privilege to restrict access and to harden cloud resources (for instance, only expose resources to the Internet as is necessary, and deactivate unneeded capabilities/features)
- All facets of computing in the cloud should use access control lists (ACL).

- Ensure privileges are role-based, and that privileged access is audited and recorded.
- if there are users from Client organization where appropriate, enable Client with administrative rights to manage or terminate access to control user access management,
- Ensure controlled access to log information as it may contain PII data.
- Just-in-time access shall be provided as per the need (business justification) /Contractual agreement) Logs shall be maintained at least for 3 years for all access provided to Users.
- Access to Cloud must be enforced with MFA.

Please refer to **Access Control Policy** for more details.

2.5 Incident Management

- All cloud security related incidents must be notified to all the appropriate stakeholders (As per IT ACT , Report to CERT-IN within six hours of any qualified cybersecurity incidents). In addition, Contractual agreements need to be considered.
- An information security incident should trigger a review, to determine if a data breach involving Personally Identifiable Information or Personal Data or Personal Sensitive Data has taken place
- Please refer to Incident Management Policy and Information Security Incident Management Response Procedure for more details.

2.6 Geographic Location for setting up cloud

As a Cloud Service Provider, Cloud based Infrastructure will be based in the following locations unless there are specific Client Requirements, if applicable

- AWS Cloud infrastructure services will be located in Singapore.
 - Azure Cloud Infrastructure services will be located in Mumbai.
- Cloud Infrastructure to be hosted in any other locations for internal organizational purposes needs to be informed to the Infosec and Data Privacy Assurance team.

2.7 Supervisory Authorities

Identify geographies and Countries where Cloud infrastructure is present and identify the Supervisory authorities.

2.8 Compliance Requirements

All functions and Projects using Cloud Computing environment must comply to the requirements of applicable Data Protection Legislations for ensuring Security and Privacy of all Informational Assets including Assets having Personal or Sensitive Data.

At least an Annual audit preferably an independent audit is to be conducted and an Annual audit report to be available for evaluating and demonstrating the compliance requirements of the processing operations on Cloud

2.9 Vulnerability Management

- Vulnerabilities must be assessed for applications.
- Cloud service team must conduct periodic vulnerability assessment internally and penetration tests from third parties and mitigation shall be done as per the Trianz Policy

- VAPT Tests shall be conducted as per Contractual Agreement
- Please refer Vulnerability Management Policy for more details

2.10 Secure Disposal

- All Cloud related assets must be disposed as per the Disposal Policy unless there are any specific Client requirements, wherever applicable
- All Cloud related assets containing Personal or Personal Sensitive Data must be disposed securely.
- Temporary files and documents must be erased or destroyed once in every six months
- All Cloud assets shall be enabled with specific retention period after which either archived/disposed basis the requirement.

Please refer to **Data Retention and Secure Disposal Policy** for more details

2.11 Logging and Monitoring Security Incidents

- Requirement for logging and monitoring must be documented. Critical events like deletion, table drop or granting privilege login must be identified and monitored independently, this can be achieved by enabling email alerts to cloud service manager and security team.
- The log details must show complete trail and must identify login name, data, time, IP address, location and activities performed.
- Health Checks shall be performed by Cloud Service Provider
- Event logs should record whether or not any Personal Data or Personally Identifiable Information has been changed (added, modified or deleted) as a result of an event and by whom.

- Define criteria regarding if, when and how log information can be made available to or usable by the Clients.
- Where Client is permitted to access log records, ensure access to records that relate to that specific Client's activities and not of others.
- Ensure controlled (Restricted) access to log information for only defined purposes when it contains Personally Identifiable Information or Personal Data or Personally sensitive Data.
- All system time must be synchronized and point to central NTP server, wherever feasible. Without such synchronization, it can be difficult to reconcile events on the cloud service systems with events and aid during investigations or maintaining the chain for custody.
- Ensure to monitor specified aspects, relevant to the cloud service and operation of the cloud services. For example, to monitor and detect if the cloud service is being used as a platform to attack others, or if sensitive data is being leaked or downloaded from the cloud service to Trianz system, monitoring identify theft.
- All the Cloud related log files must be retained at least for three years or based on Client Contractual requirements. Automated procedures must be available for ensuring this

Refer Information **Security Logging and Monitoring Policy** for more details.

2.12 Licensing requirements

- The cloud service team shall have a procedure for identifying cloud-specific licensing requirements before permitting any licensed software to be installed in a cloud service.
- Attention shall be paid to cases where the cloud service is elastic and scalable, and the software can be run on more systems or processor cores than is permitted by the license terms

2.13 Hardening

- If Trianz acts as a Cloud Service Provider Hardening shall be to protect the underlying network and infrastructure
- In case of Trianz acting as Cloud Service Customer, Trianz shall be responsible for protecting the actual data, applications, and services, which requires cloud- or servicebased security appliances like firewalls and web gateways. (also the basis of Contractual agreement)

2.14 Following must be adhered to Password Management for Privileged and Non-Privileged passwords.

-
- Never allow the use of shared passwords. Combine passwords with other authentication systems for sensitive areas like multifactor authentication. Ensure password management best practices.
- All Cloud instances and services must be discovered and grouped as part of this Asset Inventory and needs to be brought under password management.
- Shadow IT (Unaccounted) Cloud resources and passwords should not arise and proliferate.
- All Access Keys shall be regenerated on periodic basis as per Industrial standards.

2.15 Virtualization

- Ensure there is proper Lifecycle management of Virtual instances.

- Ensure Storage and access controls for virtualized instances, snapshots.
- Ensure complete Protection of Hypervisors
- Ensure that there are adequate Security Controls governing use of self-service portals.
- Ensure that access to any data previously residing is not visible to Client when Data storage space is allocated. Ensure controls in place to guarantee that only authorized snapshots are taken, and that these snapshots' level of classification and storage location and encryption is compatible in strength with the production virtualization environment •
- Ensure access to the Hypervisor administrative access logs. ☐ Ensure Hypervisor Logging is enabled.
- Below are examples of Logging that can be ensured:
- Use centralized logging: centralize logging of guest OSs, either on a separate logging system or in a repository. Use of centralized logging aids administrators, security personnel, and auditors in verifying configurations and practices in a virtualized environment (e.g., ensuring that configurations of guest OSs remain synchronized with regard to patches, updates and signatures).
 - Correlate logs: correlate server and network logs across virtual and physical infrastructures to reveal security vulnerabilities and risk.
- Regularly audit virtualized environments: it is important to audit configurations of all components of a virtualized environment, management capabilities, virtual switches, virtual and physical firewalls, and other security devices (e.g., intrusion detection systems, antimalware capabilities). Ensuring compliance with established configuration management practices is particularly important.
- Root and administrative privileges: log monthly root and administrative access and actions on all systems in a virtualized infrastructure.
 - Invalid logical access attempts: log weekly all invalid logical access attempts on all systems in a virtualized infrastructure.

- Access to all audit trails: log monthly all access to audit trails on all systems in and supporting a virtualized infrastructure (e.g., a centralized log repository).
- Initialization of audit logs: log monthly initialization of all audit logs on all systems in and supporting a virtualized infrastructure (e.g., a centralized log repository).
 - Creation and deployment of Virtual Machines (VMs): log monthly the creation and deployment of all VMs in a virtualized environment.
 - Migration of VMs: log monthly the migration (e.g., source and target systems, time, and authorization) of all VMs in a virtualized environment.
- Creation and deletion of system-level objects: log quarterly the creation and deletion of all system-level objects in a virtualized infrastructure.

2.16 Information Back up

- Ensure additional or alternative mechanisms to off-site backups for protecting against loss of data (including Personal and Personal and Sensitive Data or Personally Identifiable information), ensuring continuity of data processing operations, and providing the ability to restore data processing operations after a disruptive event.
- Multiple copies of data in physically and/or logically diverse locations (which may be within the information processing system itself) shall be created or maintained for the purposes of backup and/or recovery and restored (as per Backup and restoration policy)
- Specific requirements from individual jurisdictions if any, regarding the frequency of backups must be complied with.
- If data to be backed up contains Personal data or Personal Sensitive Data or Personally Identifiable information, it needs to be anonymized or erased as much as feasible and if there are no specific contractual Client requirements on the same For more details, please refer to Backup and Restoration Policy

2.17 Change Management

- Implement and maintain a change management process to track identified problems, fixes, and releases during the complete service life cycle for SAAS, PAAS and IAAS based services.
- Govern the impact on compliance, security, and performance of the infrastructure when VM Images are created, updated, or patched.
- Maintain consistent change management policies within the scalable and automated cloud instance provisioning systems.
- Govern changes to OS credentials when new server images are launched or terminated.
- Must monitor and manage changes in OS firewall configurations to identify anomalous or unauthorized changes. Ideally, internal configuration management solutions can integrate with Cloud instance related changes without necessitating substantial modifications.
- Infrastructure Change management becomes an ongoing process since infrastructure changes happen rapidly and with high frequency. As such, all changes should be tracked back to specific user stories. This approach ensures that the unused instance resources are terminated and therefore don't add to the cost when they are not required or running.

Please refer to the **System and Software Change Management Policy** for more details.

2.18 Cloud Service Provider Management

- As a Cloud Service Customer, need to ensure the below (as applicable):-

- Ensure the approach to patch known Vulnerabilities by Cloud Service Provider ☐ Beware of Data Backup, Retention, and Recovery Policies of Cloud Service Provider.
- Ensure to train IT staff on accessing and using the Cloud Service Provider log services.
- Ensure logging is enabled for all security events (covering sessions and transaction information) as per Industrial standards.
- Ensure that the Cloud Service Provider supports Several Multi-Factor authentication mechanisms, such as tokens, one-time passwords, biometrics...etc.
- Ensure NOT to grant the Cloud Service Provider permissions to directly use/access the organization authentication environment such as the organization's main directory.
- Ensure that we are provided at least annually with the Disaster Recovery testing reports the reports should be comprehensive, covering from the exercise scope till the final outcome and recommendations.
- Ensure that we are responsible for some or all aspects of access management for users under our control.

2.19 Roles and Responsibilities

- a) IS team must ensure the following for all internal Cloud Subscriptions and applications hosted on Cloud for internal purposes.
 - Cloud Service Provider Management for all internal Subscriptions
 - ☐ Tracking IT Assets on Cloud for internal infrastructure.
 - Security Operations Management includes but not limited to Patch and antivirus Management, Vulnerability testing, taking backups, secure disposal.
 - Encryption enablement if required.

- Identification of geographical location of hosting Cloud based on compliance requirements.
- Ensure the approval from CISO/CIO and inform Infosec/ Data privacy assurance team for deploying cloud services in any other geo-locations.
- Resource Management: Provision and manage cloud resources efficiently, including virtual machines, storage, networking, and other cloud services, to optimize costs and performance.
- Monitor and optimize the performance and availability of cloud services, including uptime, service level agreements (SLAs), and scalability for all the subscriptions on Cloud Infrastructure.
- Ensure pay-as-you-go service is effectively managed for all the subscriptions on Cloud Infrastructure.

b) Functional teams are responsible for

- Data or Information on Cloud for their respective data
- User access control
- Personal Data inventory
- Retention and secure disposal
- Encryption requirements identification

c) Cloud Delivery team must ensure.

- Cloud Service provider Management for all Client related subscriptions
- to maintain cloud asset inventory list for respective Projects
- defining and documenting agreed Roles and Responsibilities between Client and Trianz for all Cloud Security and Privacy aspects

d) Infosec and Compliance team must ensure

- Maintenance of Policy and procedure for Cloud Security and Privacy
- Monitoring and communicating any specific regulatory requirements for Cloud based environments.

- Please refer to ISAC Roles and Responsibilities document for more details
 -

3. Exceptions(s)

Any exceptions to follow **Exception Policy**.

4. ISO Control Mapping

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
Organizational Control	5.23 Information Security for use of Cloud Service	Cloud Security Policy

For Trianz Process Improvement Group (TPIG) Purpose Only

Owner:	CISO	Release ID:	CSPP-POL-058
---------------	------	--------------------	--------------

Version History

Ver. No. .	Date	Auth or	Revi ewer	Approv er	Reason for Change	Chang e Descrip tion
0.1	11- NOV- - 19	Anitha Ravindra n	Phani Krish na		Absence of such Policy and 27017 and 27018 requireme nts	Initial Version

0.2	12 - Nov - 19	Anitha Ravindran	Phani Krishna		Review comments	Updated review comments
-----	---------------	------------------	---------------	--	-----------------	-------------------------

0.3	22-Nov-19	Anitha Ravindran	Phani Krishna		Missing sections for requirements of 27017, 27018	Added Change Management and Roles and Responsibilities
1.0	25-Nov-19	Karthik		Vivek Sambasivam	Approved for Release to Blue Book	Baselined
2.0	11-May-20	Anitha Ravindran	Phani Krishna		Management Direction	Modified into new template
2.1	4-Feb-21	Vijaya Rajeswari	Phani Krishna		For Review	Updated Information Classification
3.0	4-Feb-21	Vijaya Rajeswari	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
3.0	4-Jan-22	Kruti	Vijaya	Phani Krishna	For Review	No changes

3. 1	5- May - 202 3	Vijaya, Beniyel, Rama Madhavan	Siva Krish na		For Review	Updated all sections except 2.7, 2.8 and 2.15 Migrated to new template
4. 0	5- May - 202 3	Vijaya, Beniyel	Siva Krish na	Srikant h Manten a	For Approval	Approved and Baselined
4. 1	15- Feb - 202 4	Vijaya	Balu	Srikant h Manten a	For Review	Updated the section ISO Control Mapping aligning to ISO 27001:2022
5. 0	23- Feb - 202 4	Vijaya	Balu	Srikant h Manten a	For Approval	Approved and Baselined
5. 1	14- May - 202 4	Nagarathin am	Vijay a, Beniy el and Balu		For Review	Updated the sections below: 2.6 Cloud Service deployment notification to Infosec/DPA

						2.19 Roles and Responsibilities Updated with Approval of authority for deploying services, Resource management, cloud optimization and cost optimization.
6.0	06-Jun-2024	Nagarathinam	Vijaya	Srikant h Mantena	For Approval	Approved and Baseline
6.1	2-May-2025	Vijaya	Balu			Migrated to a new Template and Yearly Review
6.0	14-May-2025	Vijaya	Balu	Srikant h Mantena	For Approval	Approved and Baseline



Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com



The content in this document is copyrighted; any unauthorized use – in part or full – may violate the copyright, trademark, and other laws. This document may not be modified, reproduced, or publicly displayed, performed, or distributed, or used for any public or commercial purposes. The Trianz name and its products are subject to trademark and copyright protections, regardless of how and where referenced.