TRIANZ℠

Policy on the use of Cryptographic Controls

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 cryptographic controls policy is to Ensure confidential information will only be received, transmitted and stored in an encrypted form.

Ensure compliance with statutory, regulatory and contractual requirements.

Authorized employees will be able to gain access when needed, to any relevant information held in encrypted form.

2. Scope

This policy is applicable to all Trianz employees, contractors, Cloud Service Providers, Cloud Service Customers and other stakeholders who are responsible for understanding and complying with this policy.

The requirements of this policy shall be implemented in all the systems under the ownership of Trianz, either on premises or on cloud and for all other Trianz managed systems, wherever applicable.

3. Roles and Responsibilities

#	Item	Roles	Responsibility
1	Cryptographic Controls	Cloud Service Provider	In case of Public Cloud PII Processor, Information on Cryptography it uses to PII Processes will be provided to Cloud Service Customer And also providing the capabilities of Cryptography used to assist Cloud Service Customer in applying its Cryptographic Controls

2	Cryptographic Controls	IS Team/ Cloud Service Customer	Ensuring the Cryptographic Controls justified by Risk Analysis In case of Cryptographic Controls offered by Cloud Service Provider need to verify whether a) Controls used are meeting the cryptography policy b) Compatible with any other cryptographic protection c) Apply to data at rest,transit and in use within the Cloud Service d) Certification Authority (CA) details to be issued

4. Policy

The confidentiality of information being imported or transferred on portable media or across networks will be protected by use of appropriate techniques such as encryption, data masking, pseudonymization or anonymization.. Encryption will be used whenever appropriate on all remote access connections to the Trianz's network and resources

Protection for data in transit

Encryption controls shall be used while transferring of confidential data over an external network to protect confidentiality of the sensitive information.

Remote access to the Trianz network:

Systems that provide access to the Trianz network from the Internet to business applications and Confidential Information must implement robust authentication methods, including passwords and encryption, to control access to information or systems

The design and installation of such systems, such as the Trianz Virtual Private Network (VPN), shall be authorized by IT to ensure that they do not provide a route for unauthorized access to Trianz information assets.

Data Storage /Data at Rest:

Data while stored/archived shall be protected appropriately based on the classification. Ideally data should be encrypted but depending on the sensitivity of data, other access controls might suffice Data in Processing:

- Data must be protected using encryption while systems are processing the data, as applicable Key Management:

The following should be considered when implementing data masking techniques:

1. not granting all users access to all data.
2. Use of obfuscated data in certain cases.
3. any legal or regulatory requirements

The following should be considered when using data masking, seudonymization or anonymization:

1. level of strength of data masking, pseudonymization or anonymization according to the usage of the processed data;
2. access controls to the processed data;
3. agreements or restrictions on usage of the processed data;
4. prohibiting collating the processed data with other information in order to identify the PII principal;
5. keeping track of providing and receiving the processed data

- All the encryptions keys must be securely stored and access to the key should be strictly restricted as defined by the access control policy.
- All the encryption keys must be changed periodically as per the requirements of their use in protecting the systems and information.
- Trianz may use RSA secure ID tokens based on two factor authentication for accessing client applications, as required by client.

- User is personally responsible for the secure use and protection of his private key.
- IS team shall be custodian of the RSA tokens.
- Trianz shall follow best practices for Encryption.

5. Reference

- Guidelines for Information Labeling and Handling
- ISO 27001:2022

6. Exception(s)

None, as of now. Exceptions to the Cryptographic controls policy shall follow the Exception handling policy

7. ISO Control Mapping(s)

Category of Control	**ISO 27001:2022 Control**	**Document Name as per ISO 27001:2022**
Technological Controls	8.24 Use of cryptography Control Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	Policy on the use of Cryptographic Controls

Document Control

Owner:	CISO	**Release ID:**	CCS-POL-0024

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
1.00	09-Jan-14	Srilakshmi	_	_	None	Initial release to Blue Book
2.00	16-May-15	Sudharsana	_	_	Upgrading to ISO 27001:2013	• Added transfer of data • Remote access to the trianz network • Key management
2.01	25-Jan-16	Balu Nair	_	_	Client Audit and alignment with shared assessment checklist.	Data Storage
3.00	08-Feb-16	Balu Nair	_	_	Approved by Mahesh (CISO)	Baselined
3.01	29-Apr-19	Balu Nair	Joshy VM	_	Annual Review	• Minor changes to the contents, Information classification modified

4.0	14-May-19	Balu Nair	_	Ganesh Arunachala	Approved for Release	Baselined
5.0	23-Nov-19	Vijaya R	Phani Krishna	Vivek S	Updated to align to ISO 27017 and ISO 27018 Standard	Updated to align to ISO 27017 and ISO 27018 Standard
5.1	12-May-20	Balu Nair	Phani Krishna			Migrated to New Template
6.0	14-May-20	Balu Nair	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
6.1	18-Jan-2021	Karthik N	Phani Krishna		For Review	Updated the information classification and format changes.
7.0	18-Jan-2021	Karthik N	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
7.0	3-Jan-22	Divya	Balu Nair		Annual review	No changes
7.1	10-Mar-2023	Beniyel S, Rama M	Balu Nair		For review	Incorporated CA as cryptography standard New template change
8.0	09-May-23	Beniyel S	Balu Nair	Srikanth M	Annual review	Approved and Baselined

8.1	19-Jan-24	Aishee G, Beniyel S	Balu Nair, Vijaya R		For Review	Policy statement has been modified. Migrated from standard ISO 27001:2013 to ISO 27001:2022 ISO Control Mappings has been updated.
9.0	23-Feb-24	Aishee G, Beniyel S	Balu Nair, Vijaya R	Srikanth M	For Approval	Approved and Baselined
9.1	06-May-25	Balu Nair	Vijaya R		Year Review	Migrated to a new Template
10.0	14-May-25	Balu Nair	Vijaya R	Srikanth M	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com