TRIANZ℠

Encryption Key Management 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 guidance for managing secured encryption for the keys using Key Management Systems (KMS) in the Cloud, On-Prem, External, Internal platforms.

2. Objectives

The objective of Encryption Key management Policy is to facilitate effective implementation of the security controls for the Keys used/implemented in the Trianz Managed environment.

3. Scope

This policy document covers the Encryption Key Management for the Trianz Managed environment.

4. Key Fundamentals:

- **Symmetric (or Secret) Key Cryptography:**

  The sender encrypts the data with the secret key and the receiver can recover the data through decryption using the same secret key. The symmetric key provides Confidentiality and Integrity of the data shared.

- **Asymmetric (or public) key cryptography:**

  This form of cryptography characterizes itself by each user in a network owning a private – public key pair. The public keys are made available to all users of the system, while the private keys are kept secret by their respective owners. User B wishing to send confidential data to user A can then use A's public key to

send the data encrypted, and only A will be able to decrypt the data with his/her private key. The Asymmetric key provides integrity and authentication.

- **Key Hierarchy:**

  Key hierarchy is a way to organize encryption keys so that a master key is used to encrypt other keys that are in turn used to encrypt the actual data want to protect.

- **Key Hierarchy types:**
  - Data encryption key (DEK): A key used to encrypt data in symmetric algorithm
  - Key encryption key (KEK): A key used to encrypt, or wrap, a data encryption key in Symmetric algorithm. To be split into two or more components protected by Split knowledge
  - Master Key: The key used to encrypt the key encryption keys (KEK). This key is securely stored on KMS Systems. Key is responsible for encrypting the keys. Not accessible in clear text for any individuals.

- **Key Strength:**

  Refer NIST SP 800-57 (Recommendation for Key Management) for guidelines on key strength for implementation. Establish application's minimum computational resistance to attack. The minimum computational resistance to attack shall take into consideration the sophistication of organization's adversaries, how long data needs to be protected, where data is stored and if it is exposed.

5. Policy Statement

Key Basic Security Principles:

- The confidentiality of all secret keys, integrity & authenticity of all keys shall be ensured
- Secret keys shall only exist as one or more of the following:
    - Within approved Secure Cryptographic Module (SCM)
    - Encrypted using KEK (Key Encryption Keys) during exchange
    - Split into multiple components protected by Split knowledge/dual control
- Individuals shall not be permitted to access any plaintext secret key
- Keys shall be generated using processes/ceremonies that does not allow for the prediction of any resulting value or the determination that certain values are more probable than others from the total set of all possible values.
- Procedures shall be in place for the timely replacement of keys in case of expiring or key compromised
- A key shall not be used when it is known or suspected to be compromised. The usage of a compromised (or suspected) key shall be terminated as soon as allowed by the technical, operational and business requirements and limitations.
- Test keys shall be prohibited from being used in production systems and production keys shall be prohibited from being used in test systems.
- Keys shall not be shared between cryptographic modules used in production and test systems.

- There shall be a process in place for the switching of cryptographic modules from test mode to production mode, and from production mode to test mode when using third party Cloud Key Management systems.

Key Implementation guidelines:

- Individual procedures to be maintained for the applications/products were used.
- The procedure shall include algorithm, key length, justification for key length, key expiry period, KMS/Cryptographic module used to protect the key, number of components split, owners of the split components, any other special controls implemented.
- Secure Cryptographic modules which are hardware, software or firmware shall be used for the key management.
- The modules shall comply with one or more below standards:
    - FIPS 140 - Security Requirements for Cryptographic Modules
    - Common Criteria (ISO/IEC 15408) - using an approved Protection Profile and Target of Evaluation.
    - Hardware Security Module (HSM) Security requirements – If any card data complying to PCI standard card is to be secured.

Key Management processes:

5.3.1 Key Generation

- Cryptographic keys shall be generated within an approved cryptographic module and with an approved key generation process.
- The process shall be such that it does not allow for the prediction of any resulting value or the probable value from the total set of possible values.

- The key management role holders and security options for the cryptographic key generation ceremony are handled as defined in the Encryption key management policy.
- The generation of cryptographic keys within a cryptographic module shall occur in a secure environment that ensures that unauthorized access or viewing is prevented.

5.3.2 Key Rotation

- *Key rotation* is the process of periodically retiring an encryption key and replace by using a new cryptographic key with minimal or no downtime.
- Periodically and automatically rotating keys is a recommended security practice and some industry standards like PCI warrants regular rotation of the keys.
- The data that is encrypted in with previous key vesions will not be automatically re-encrypted. Ensure there's no data loss/service unavailability during the rotation.
- Do follow the guidelines provided by KMS for re-encrypting the data with the new key-pair used in the rotation

Key Revocation

- Ensure the below when a key is revoked:
    - All related/relevant parties are informed.
    - All instances of the key are revoked.
    - Keys that are encrypted with the revoked key are also revoked.
    - Revoked keys shall not be returned to backup use.

Key Disposal/Destruction

- Only keys that have been revoked or compromised can be disposed.
- Reconstruction or recovery of a key after disposed is not allowed
- Key destruction shall be witnessed and logged under dual control.
- If a key that resides inside a cryptographic module cannot be disposed, then the module itself shall be disposed in secured manner that no residual trace of stored key remains
- Whenever a KMS/cryptographic module is permanently removed from service, all of its resident keys shall be securely destructed/disposed

Key Activation

- Key to be used to cryptographically protect information or process previously protected information.
- The use of each Active keys are to be duly recorded

Key Deactivation

- An active key may transition to deactivate state if identified as integrity of the key is compromised or past the agreed cryptoperiod.
- Deactivated Key need to be replaced with another new generated key in active state

Key Archival

- Archival of a key is only permitted if specified for use in the application product procedure
- An archived cryptographic key shall only be used to verify the legitimacy of data resulting from its application that occurred prior to archiving

- An archived cryptographic key shall have its explicit tagging information modified to only permit the usage of the key for verification purposes.
- Copies of retired cryptographic keys that are to be archived shall be stored in a separate location from any active keys
- Archived cryptographic keys shall be stored in accordance with the same standards as active or backup keys
- All archived keying material shall be stamped with a non-modifiable time stamp when moved to archive.
- Retention period of archived keys shall be determined based on business need

Key Compromise

- Keys are considered as compromised based on following:
    - Identified as key got exposed or identified in a security investigation
    - A stored key or distributed key fails an integrity check
    - Key managed cryptographic module shows signs of compromise or lost or stolen
    - A key higher in the hierarchy is compromised
    - A breach in segregation of duties, dual control, or access controls is identified
    - The plaintext value of the key has been exposed.
- If the compromised key is KEK or a master key from which other keys are derived, then all keys hierarchically under it shall also be revoked and replaced

- If the compromised key is a working key, then data associated with such key shall be revoked and re-encrypted with new working key in accordance with the policy
- There shall be investigation triggered including Infosec team on any key compromise followed by root-cause and remediations detailed

Key Recovery

- Key stored in the Systems may sometimes be corrupted which would need keys to be recovered from the backup securely.
- Keys to be replaced earliest with new keys in accordance with technical, business up-time requirements.
- The backup copies of the cryptographic keys are to be secured as similar to operation keys.

Key Inventory

- All long-term keys are to be inventoried including the owners/sponsors, application used, used to protect data in transit/in store details etc.,
- Key inventory shall tag unique reference of each key in the system.
- Key inventory shall be protected and stored in centralized repository
- Key inventory shall have details of the cryptoperiod and mechanism to inform owner for replacement earlier to the expiry.

6. Key Logging & Audit Trail:

- Key management logs shall contain The unique identifier of the key or specific key instances, Date of the activity, action taken (e.g., key generation, key distribution, key disposal, etc.)

- Log shall record date-time stamp, sequence number, event record.
- Log shall include any operator logon/logoff, key management activities using secrets/cards etc.,
- Audit trails to be maintained for all the key activities.
- Audit trails to be backed up for future references.
- KMS system shall have facility to troubleshoot audit log validation errors.

7. Roles & Responsibilities

Roles	Responsibilities	Internal/External
Project/Product Security, Cloud, Infra management team	Adhere to the Encryption Key management policy	Internal
Product Owner /Project Manager/Operations Manager	Validate the Encryption key management is done based on the policy	Internal
InfoSec & Compliance Team	Validate the key management process iis adhered as per the policy	Internal

8. Applicable Standards

- ISO 27001:2022
- ISO 27701:2019
- NIST.SP.800-57
- FIPS 140-2

9. Exception(s)

There is no exception to this policy.

10. ISO Control Mapping

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
Technological Controls	8.11 Data masking Control Data masking shall be used in accordance with the organization's topic specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration	Encryption Key Management Policy

Document Control

Owner:	CISO	**Release ID:**	KEM-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 Mar 22	Divya	Balu Nair	Siva N	Initial Version	None
1.0	25th Mar 22	Divya	Balu Nair	Siva N	Baselined	Baselined
1.1	29-Marh-2023	Krutideepta	Vijaya R	Srikanth M	For Review	Reviewed with no changes
1.2	12-May-2023	Rama Madhavan	Vijaya		For Review	Migrated to new template
2.0	12-May-2023	Rama Madhavan	Vijaya	Srikanth M	For approval	Approved and Baselined
2.1	15-Feb-24	Shalini	Vijaya		For Review	Mapped with new ISO 27001,2022 control 8.11
3.0	23-Feb-24	Shalini	Vijaya	Srikanth	For Approval	Approved and Baselined
3.1	06-May-25	Balu Nair	Vijaya		Yeary Review	Migrated to a new Template
4.0	14-May-25	Balu Nair	Vijaya	Srikanth M	For Approval	Approved And Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com