Cryptography, Encryption & Key Management Policy

Version 2

REZOLVE.ai

Document Information

Name of the document	Cryptography, Encryption & Key Management Policy
Release date	23-May-2025
Owned by	Neil Dattani
Governed by	Udaya Bhaskar Reddy

Revision History

Version No	Version Date	Details of Change
1	21-May-2025	Initially Drafted
2	22-May-2025	Final

Reviewer and Approver

Name	Title	Comments	Date Reviewed
Mr.Udaya Bhaskar Reddy	Co-Founder & CTO	Approved	23-May-2025

Contents

1. Purpose

This policy establishes requirements for the secure use of cryptographic controls, data encryption, and key management within our SaaS platform to:

- Protect customer and internal sensitive data
- Ensure compliance with security standards (e.g., SOC 2, ISO 27001, GDPR)
- Reduce risk from key compromise, improper use, or insecure storage

2. Scope

This policy applies to:

- All production systems and environments hosted on Azure
- All internal and tenant-scoped secrets, tokens, and credentials
- All cryptographic keys used to encrypt data at rest or in transit

3. Cryptographic Principles

- **Encryption at Rest:** All sensitive data is encrypted using AES-256-GCM.
- **Encryption in Transit**: TLS 1.2+ is required for all inter-service and client communication.
- **Envelope Encryption**: Data is encrypted using a Data Encryption Key (DEK), which is itself encrypted with a Key Encryption Key (KEK) managed in Azure Key Vault (AKV).
- **Key Separation:** DEKs are unique per (tenant_id, integration_id) for tenant data, and per secret name for internal secrets.
- **Key Rotation**: Keys are rotated periodically based on classification and threat level

- Employees must report loss or theft of any device within 4 hours.
- IT/Security will trigger remote wipe and revoke access where possible

4. Key Management Roles & Responsibilities

Role	Responsibilities
Security Team	Define crypto standards, approve changes, audit usage
Engineering Team	Implement encryption mechanisms, integrate with AKV
DevOps	Manage Azure Key Vault configurations and key lifecycle
Auditor (internal/external)	Validate compliance with this policy and crypto controls

5. Key Types & Usage

Key Type	Description	Use
KEK	Key Encryption Key managed in Azure Key Vault (RSA-2048 / RSA-OAEP)	Encrypts DEKs
DEK	Data Encryption Key (AES-256-GCM) generated per tenant-integration or secret	Encrypts tokens/secrets

Key Type	Description	Use
TLS Certificates	Issued and renewed via automated providers (e.g., Azure-managed or Let's Encrypt)	HTTPS, mTLS

6. Key Lifecycle Requirements

6.1 Key Generation

- DEKs are generated using cryptographically secure random generators (crypto.randomBytes)
- KEKs are created and stored securely in Azure Key Vault using RSA-OAEP

6.2 Key Usage

- DEKs are never stored unencrypted
- KEKs are never exposed outside AKV

6.3 Key Rotation

- KEKs: Rotated annually or upon compromise
- DEKs: Rotated when:
    - Tokens are regenerated
    - DEK compromise is suspected
    - Integration ownership changes

6.4 Key Revocation & Deletion

- KEKs are soft-deleted and purged in AKV
- DEKs are rotated and old values are overwritten in the database
- Expired tokens are cleaned up on a schedule (TBD)

7. Key Storage

Storage Medium	Security
Azure Key Vault	Stores KEKs, enforces RBAC, logs access
PostgreSQL DB	Stores DEKs encrypted with KEKs, access tightly scoped
Kubernetes Secrets (legacy)	Being phased out; only for bootstrap configs

8. Logging, Auditing & Monitoring

- All access to Azure Key Vault is logged via Azure Monitor & Activity Logs
- Token usage, rotation, and access are logged in the app audit trail
- Key lifecycle events (generation, encryption, decryption, deletion) are logged
- Policy reviewed annually or after any key-related security event

9. Monitoring, Auditing, and Lifecycle Management

9.1 Encryption System Audits

Encryption and key management systems must be audited at least annually, and immediately following any security incident that could impact the confidentiality, integrity, or availability of cryptographic assets.

- Audit logs include: key creation, activation, rotation, revocation, deletion.
- Azure Key Vault diagnostics and access logs are retained and reviewed.
- Internal tooling flags key rotation delays and abnormal decryption usage.

9.2 Secure Key Destruction

All keys deemed obsolete (e.g., due to tenant offboarding, rotation, or compromise) are to be securely destroyed.

- DEKs stored in DB are securely deleted by zeroing encrypted fields and removing the encrypted blob.
- KEKs stored in Azure Key Vault are deleted and then purged after soft-delete period.
- Destruction processes must be logged and reviewed.

9.3 Continuity vs. Key Loss Risk Management

We assess trade-offs between operational continuity and risk of key compromise:

- Backup/recovery strategy prioritizes KEK availability.
- DEKs are only needed for on-demand decryption; not stored in plaintext.
- In the event of KEK loss, encrypted data is considered unrecoverable unless securely backed up.
- This risk is acknowledged, and affected data is re-ingested or requested from source systems.

9.4 Internal Monitoring and Reporting

Cryptographic operations and controls are monitored and internally reported as follows:

- Weekly reports flag failed decryption attempts and anomalies in token use.
- Changes to key-related configuration (AKV key rotations, new DEK generation) are logged.
- Internal dashboards track DEK age, KEK rotation history, and tenant/integration health.

9.5 Key Lifecycle Logging and Audit

Key lifecycle events are logged and monitored to enable forensic traceability and compliance:

- Events tracked: create, use, rotate, revoke, delete
- Logs are stored in centralized logging stack (e.g., Azure Monitor, or Elastic)
- Alerts raised on:
    - Unusual access to KEK
    - Frequent decrypt operations on expired/disabled DEKs
    - Failed encryption/decryption operations

9.6 Key State Transitions

All key transitions — including activation, suspension, revocation, and deletion — are:

- Logged with a timestamp, user/actor, and purpose.
- Reviewed biweekly by Security/DevOps leads.

- Marked in metadata in the key inventory (e.g., active, revoked, archived).

10. Incident Response

If any cryptographic key is suspected to be compromised:

- Revoke or rotate the key immediately
- Trigger emergency token invalidation
- Notify affected parties if required (based on severity)
- Log and review incident as part of post-mortem

11. Policy Review

- Reviewed at least **annually**
- Updated upon:
    - Significant architecture changes
    - New regulations or compliance frameworks
    - Post-incident recommendations

Appendix A: Approved Algorithms

Use Case	Algorithm
DEK	AES-256-GCM
KEK	RSA-OAEP (2048+ bits)
Random	CSPRNG (Node.js crypto.randomBytes)
Transit	TLS 1.2+

Appendix B: External Tools Used

Tool	Purpose
Azure Key Vault	Secure KEK storage & crypto ops
Node.js crypto	DEK generation, AES-GCM encryption
PostgreSQL	Encrypted token storage
GitHub Actions (planned)	Secret rotation automation
Notion/Excel (planned)	Key inventory & audit tracking

NOTE – Next review cycle for this policy is **March 2026**.
Management can review the policy at any time and can make changes depending on the situation.

All documents related to policies and procedures - any reference to Actionable Science is as good as Rezolve.ai.