

PAPER TIGER TECHNOLOGIES

Encryption and Key Management Policy

1. Purpose

The purpose of this Encryption and Key Management Policy is to define where encryption is required in the PaperTiger environment and how the keys that protect data are generated, stored, rotated, and destroyed. Encryption is only as strong as the discipline around its keys.

A common failure is to encrypt data but leave the keys sitting next to the ciphertext, which defeats the purpose. This policy therefore treats key management as the harder and more important half of the problem, and ties encryption requirements to the data classification scheme.

This policy is fictional and illustrative. It describes no real key, certificate, or cryptographic operation.

The policy treats key management as the harder and more important half of the problem: encryption is only as strong as the discipline around its keys, and a robust cipher with mishandled keys offers little protection.

Encryption only protects data when the keys are controlled, so the policy treats the algorithm and the key as a single unit and governs both together.

Encryption is a moving target, so the policy does not just encrypt once; it keeps keys versioned and algorithms current so the protection does not quietly rot.

Encryption exists to protect data whether it is moving or at rest, and key management exists so the protection is not undone by a lost or long-lived key.

2. Definitions

Term	Definition (illustrative)
Encryption	The transformation of data so it is unreadable without the corresponding key.
Key	The secret value used to encrypt and decrypt data.
Key custodian	The role that performs key generation, rotation, and escrow.
Data at rest	Stored data on disks, volumes, or backups.
Data in transit	Data moving across a network.
Certificate	A public credential that binds an identity to a

	key.
Rotation	The scheduled replacement of a key or certificate.
Managed store	The controlled location where keys are generated and held.
Key escrow	The controlled recovery copy of a key.
Destruction	The irreversible removal of a key so ciphertext cannot be decrypted.
Algorithm standard	The documented list of approved algorithms and key lengths.
Duty separation	The split between key generation and key use approval.
Key audit	The periodic comparison of usage to the inventory.
Encryption at rest	The protection applied to stored data so a stolen or copied store is unreadable without the key.
Encryption in transit	The protection applied to data moving between systems so it cannot be read in flight.
Key ceremony	A controlled, witnessed procedure for generating or recovering high-value keys.
Key version	A specific generation of a key, tracked so rotation and revocation can be applied precisely.
Crypto agility	The ability to switch algorithms or key lengths when a standard is weakened.
Key rotation	The scheduled replacement of a key with a new one.
Algorithm agility	The ability to move to a stronger algorithm as guidance changes.
Key inventory	The list of keys with owners, algorithms, and rotation dates.
Hardware security module	The device that protects keys in tamper-resistant hardware.
Certificate authority	The issuer of digital certificates.
Cipher suite	The named set of algorithms for a connection.
Cryptography	The science of protecting data through encoding.
Key management	The lifecycle control of cryptographic keys.
TLS	The protocol that encrypts data in transit.
Certificate rotation	The renewal of a certificate before it expires.

3. Scope and Boundaries

This policy applies to fictional data at rest and in transit, and to the cryptographic keys and certificates used inside the illustrated service boundary. It covers customer data, internal data, and backups alike.

It applies to every system that stores or transmits sensitive data, and to the keys that protect those systems, regardless of where the key lives.

Out of scope are real data, real keys, and real cryptographic systems. This policy creates no real obligation and asserts no certification.

The scope includes backups on equal footing with live data, because a backup is just data at rest in another location and is a common place for encryption discipline to lapse.

Escalation for a key or algorithm issue follows a fixed chain: a suspected compromise goes to the key custodian, then to the Information Security Lead, and finally to the governance forum when a root or high-value key is affected.

Encryption protects customer data at rest and in transit; the key-management rules apply to every key in the demonstration, including internal ones.

Encryption is fictional and applies to the demonstration's data at rest and in transit.

4. Roles and Responsibilities

Role	Illustrative responsibility
Cryptography Lead	Owns the policy and the key inventory.
Key Custodian	Performs key generation, rotation, and escrow.
Platform Team	Applies encryption settings to systems and data stores.
Application Team	Implements encryption in application code.
Security Operations	Monitors key access and certificate expiry.
Trust Center Coordinator	Maintains the fictional label on shared copies.

The following RACI is illustrative.

Illustrative RACI for key lifecycle:

Activity	Key Custodian	Cryptography Lead	Platform Team	App Team
Generate keys	R	C	I	I
Apply encryption	I	C	R	R
Rotate keys	R	A	C	C
Escrow keys	R	A	I	I

Destroy keys	R	A	I	I
--------------	---	---	---	---

5. Policy Requirements and Controls

PTT-POL-008-C01. Encrypt data in transit

Data crossing untrusted networks uses current transport encryption, so that an observer on the wire cannot read customer or internal data. A scan confirms no service accepts a deprecated protocol.

PTT-POL-008-C02. Encrypt data at rest

Stored customer and internal data is encrypted in the demo, so a stolen disk or exposed volume does not by itself expose the data. A report lists any store without encryption.

PTT-POL-008-C03. Use approved algorithms

Only current, recognized algorithms and key lengths are permitted, because legacy algorithms weaken the entire chain regardless of how carefully keys are managed. A scan rejects a weak algorithm at configuration time.

PTT-POL-008-C04. Separate keys from data

Keys are stored apart from the data they protect, in a managed store, so that compromising the data store does not also compromise the keys. The key and the ciphertext are stored apart, so one breach does not yield both.

PTT-POL-008-C05. Rotate keys on a schedule

Keys and certificates are replaced before expiry or compromise, limiting the useful life of any single key. The rotation log is checked against the schedule.

PTT-POL-008-C06. Control key access

Key access is limited to the key custodian role and is logged, so that any use of a key is attributable. Key access is logged and sampled.

PTT-POL-008-C07. Destroy keys securely

Retired keys are destroyed so old ciphertext cannot be decrypted, closing the loop at the end of a key's life. A retired key is destroyed so it cannot be used to decrypt old data.

PTT-POL-008-C08. Manage certificates

Certificates are inventoried and replaced before expiry so that services do not fall back to insecure or self-signed states. Certificate expiry is tracked and a renewal is scheduled before lapse.

PTT-POL-008-C09. Escrow with control

A recovery copy of keys is escrowed under the same access controls, so recovery is possible without a bypass. Escrowed keys are stored under split control, so no single person can recover them.

PTT-POL-008-C10. Respond to key compromise

A suspected compromised key is revoked and replaced through the incident process, and the affected data is re-encrypted.

PTT-POL-008-C11. Maintain an algorithm standard

The approved algorithms and key lengths are listed in a documented standard, so engineers do not each make their own crypto decisions. The standard is reviewed annually as recommendations evolve. The standard names the allowed algorithms and key lengths.

PTT-POL-008-C12. Separate duties for keys

The person who generates keys is not the person who approves their use, so no single role controls a key end to end. Key creation and key use are held by different roles.

PTT-POL-008-C13. Audit key usage

Key usage is audited against the approved inventory, so a key used outside its purpose is detected rather than assumed legitimate. The usage log is sampled monthly.

PTT-POL-008-C14. Encrypt backups

Backups are encrypted at the same level as the data they copy, so a lost backup does not expose the data. Backups are encrypted with the same discipline as the primary data.

PTT-POL-008-C15. Manage key lifecycle end to end

Keys are managed from generation through rotation to destruction, so no stage of the lifecycle is left to ad hoc handling. Each key has a known state from creation through rotation to destruction.

PTT-POL-008-C16. Document cryptographic exceptions

Any deviation from the crypto standard is documented, so an exception is a decision rather than a lapse. An exception is documented with its reason and its review date.

PTT-POL-008-C17. Track key versions

Each key carries a version and a status, so a key can be rotated or revoked precisely rather than by guesswork. The version history is the record of when and why keys changed. A key's version is recorded, so the right key is used to decrypt the right data.

PTT-POL-008-C18. Maintain crypto agility

The environment can move to a new algorithm or key length on a defined plan, because a standard that is secure today can be broken tomorrow, and the migration should not be a crisis. The design allows a move to a stronger algorithm without a rebuild.

PTT-POL-008-C19. Prohibit weak or deprecated algorithms

Algorithms and key lengths known to be weak are not used for new data, and legacy uses are scheduled for migration, so no data rests on a standard already shown to be breakable. A weak algorithm is blocked, not merely discouraged.

PTT-POL-008-C20. Conduct key ceremonies for high-value keys

Generation and recovery of the highest-value keys occurs in a witnessed ceremony with a defined quorum, so no single person controls a root key. A high-value key is handled in a witnessed ceremony with multiple people present.

PTT-POL-008-C21. Document the key inventory

Every key is listed with its owner, algorithm, and rotation date, so the key estate is known rather than scattered across systems. The inventory is reconciled against the vault.

6. Operating Procedures

Inventory keys.

The Cryptography Lead records every key and certificate with its owner and expiry.

Generate in the managed store.

Keys are created in the approved store, never on ad-hoc devices or in code repositories.

Apply to new stores.

New data stores are encrypted before first use, and the encryption is verified.

Rotate before expiry.

Keys and certificates are replaced on their scheduled interval.

Escrow the recovery copy.

A recovery copy is placed in escrow under access control.

Recover for incident.

Compromised keys are revoked and replaced as part of the incident process.

Destroy at retirement.

Retired keys are destroyed and the destruction is recorded.

Monitor expiry.

Security Operations monitors certificate and key expiry and raises alerts.

Review the algorithm standard.

The Cryptography Lead reviews the approved algorithm list annually and updates it as recommendations change.

Audit key usage.

A periodic audit compares key usage against the inventory and flags anomalies.

Encrypt a backup.

Backups are encrypted before transfer and storage.

Document an exception.

A crypto deviation is documented with its rationale and date.

Rotate a data key.

The owner schedules the rotation, the new key is generated in the controlled store, and the rotation is recorded with the affected scope.

Hold a key ceremony.

The required witnesses assemble, the procedure is followed step by step, and the outcome and attendees are recorded.

Retire a deprecated algorithm.

Uses of the weak algorithm are identified, migrated to an approved one, and the retirement is recorded.

Revoke a compromised key.

The key is marked revoked, affected data is re-encrypted under a new key, and the revocation is recorded.

Rotate a key.

The owner generates the replacement, updates the systems that use it, and records the rotation.

Respond to a compromise.

The owner revokes the compromised key, issues a replacement, and reviews what the key protected.

Rotate a certificate.

The owner renews the certificate before expiry and updates the services that use it.

Destroy a retired key.

The owner destroys the key and records the destruction in the inventory.

Run a key ceremony.

The operators handle the master key in a witnessed procedure and record the event.

7. Frequency and SLAs

Illustrative crypto cadence:

Activity	Frequency (illustrative)
Key rotation	Annually or on compromise
Certificate renewal	Before expiry
Key inventory review	Quarterly
Algorithm review	Annually

8. Exceptions and Lifecycle

An exception permits a short delay in rotating a legacy key when the Cryptography Lead documents the residual risk and adds monitoring. The exception names the key and the new rotation date.

Exceptions are time-boxed and reviewed quarterly. A key that remains unrotated past its exception window is escalated as a finding.

A key that remains unrotated past its exception window is escalated as a finding, because an overdue rotation is a concrete, measurable gap rather than an abstract concern.

9. Records and Evidence

Record type	What it demonstrates (illustrative)
Key inventory	The list of keys and certificates with owners and expiry.
Rotation records	The scheduled replacements.
Encryption configuration records	The applied at-rest and in-transit settings.
Key access logs	The recorded use of keys.

Destruction records	The recorded key destruction.
Certificate inventory	The managed certificates.
Algorithm standard	The approved list with its review date.
Key usage audit	The comparison of usage to the inventory.
Ceremony records	The witnessed generation and recovery events.
Cipher suite list	The approved suites per service.
Key management records	The documented key lifecycle events.
TLS configuration	The approved protocol settings per service.

10. Oversight and Metrics

- Encryption coverage: 100 percent of sensitive stores encrypted (illustrative).
- Rotation compliance: 100 percent of keys rotated within window.
- Certificate expiry: zero expired certificates in production.
- Key compromise: each compromise handled within the incident window.
- Algorithm compliance: 100 percent of keys use an approved algorithm.
- Encryption coverage: the share of sensitive stores and paths encrypted trending to 100 percent.
- Key rotation timeliness: keys rotated within their defined window.
- Percentage of keys rotated within their schedule.
- Number of keys past their rotation date.
- Percentage of keys rotated within schedule.
- Certificates renewed before expiry.
- Deprecated ciphers disabled across services.
- Keys past rotation.
- Services on a deprecated protocol.

11. Appendix

Illustrative encryption scope:

Scope	Approach (illustrative)
Data in transit	Transport encryption for public endpoints
Data at rest	Storage encryption for customer and internal stores
Backups	Encrypted before transfer and storage

12. Related Policy Dependencies

- Data Classification and Handling Policy (defines which data must be encrypted)
- Secure Configuration Policy (enforces the crypto settings on systems)
- Business Continuity and Disaster Recovery Policy (protects encrypted backups)

- Incident Response Policy (governs key compromise response)
- Identity and Authentication Policy (governs the credentials that protect key access)

13. Review Cadence

The Cryptography Lead reviews this policy at least annually, after a change to the illustrated crypto stack, and after any significant simulated key compromise.

Revision History

Version	Date	Change summary	Author
1.0	September 28, 2026	Original enterprise-depth fictional demo policy for controlled trust-center testing.	Paper Tiger Technologies

Document Control

Field	Value
Document ID	PTT-POL-008
Document Owner	Cryptography Lead
Status	Fictional demo artifact
Effective Date (illustrative)	September 28, 2026
Review Cadence	At least annually and after material fictional changes
Classification	Internal Demo
Approval	Illustrative governance approval only; no real adoption represented