

PAPER TIGER TECHNOLOGIES

Asset Management Policy

1. Purpose

The purpose of this Asset Management Policy is to establish how Paper Tiger identifies, owns, tracks, and disposes of the information assets in the illustrated environment. A reliable inventory is the foundation for classification, patching, incident response, and every other control that assumes you know what you have.

An asset you cannot see you cannot protect. The inventory is what lets the vulnerability program know what to scan, the patch program know what to update, and the incident team know what to contain. This policy therefore treats the inventory not as an administrative nicety but as the substrate of the whole security program.

This policy is fictional and illustrative. Paper Tiger Technologies and the PaperTiger platform are fictional, and no statement here describes a real asset, facility, or system.

The inventory is the substrate of the whole security program: the vulnerability program scans it, the patch program updates it, and the incident team contains it. A program built on an inaccurate inventory is doing precise work on the wrong objects.

Every security control presumes the organization knows what it has, so the asset policy builds and maintains that knowledge as the foundation the rest of the program stands on.

The inventory only earns its keep if it drives decisions, so the policy layers criticality and dependency on top of the raw list and uses both to set priorities.

Asset management exists so every system is known, owned, and protected, and the policy makes the inventory a living record rather than a one-time list.

2. Definitions

Term	Definition (illustrative)
Asset	Any illustrated device, system, service, data set, or repository inside the service boundary.
Asset owner	The role accountable for an asset's classification, status, and disposition.
Asset Steward	The role that owns the policy and the master inventory.
Inventory	The authoritative record of assets with identifiers, owners, and classifications.

Discovery	The process of detecting assets that may not yet be in the inventory.
Baseline	The minimum security configuration an asset must meet before use.
Disposition	The end-of-life treatment of an asset, including transfer or sanitization.
Sanitization	The destruction of data on media so it cannot be recovered.
Lifecycle	The stages an asset moves through from acquisition to disposition.
Unmanaged asset	An asset found in the environment but not under inventory control.
Criticality tier	The ranked importance of an asset to the service.
Relationship map	The recorded dependencies between assets.
Procurement reconciliation	The comparison of inventory to purchasing records.
Configuration management database (CMDB)	The inventory that records each asset, its owner, its location, and its relationships.
End of life	The point at which an asset no longer receives vendor support or is retired from the demonstration.
Critical asset	An asset whose loss or compromise would materially damage the demonstration, and which therefore receives the highest care.
Asset inventory	The maintained list of everything the provider runs.
Decommission	The formal removal of an asset from service.
Asset relationship map	The documented dependencies between assets.
Configuration management database	The system of record for assets and their relationships.
Software bill of materials	The inventory of components in a software asset.
Software license	A grant to use a software product under stated terms, including the number of permitted installations or users.
Cloud resource	A provisioned compute, storage, or service instance running in a cloud environment.

3. Scope and Boundaries

This policy applies to fictional endpoints, cloud resources, software services, repositories, and removable media inside the service boundary. It covers both company-managed and customer-facing assets that store or process demo data.

It applies to the full lifecycle: acquisition, registration, use, transfer, and disposition. Every stage has a record so the inventory stays current as assets move through their life.

Out of scope are real devices, systems, and data. This policy describes no real hardware, no real facility, and no real disposal event.

Customer-facing assets are in scope on equal footing with internal ones, because a customer-facing asset that falls out of the inventory is the one most likely to be attacked and least likely to be patched.

The escalation for an asset issue follows a fixed chain: an unowned or unsupported asset is flagged to the asset administrator, then to the Information Security Lead if the asset is critical, and finally to the governance forum when the asset represents a material risk.

The inventory is the demonstration's own asset picture and is fictional.

The inventory feeds the continuity plan and the patch program, so an asset that is not on the list is invisible to every other control that depends on it.

This policy covers physical hardware, virtual machines, containers, and software assets, whether purchased, leased, or provisioned through a cloud subscription.

4. Roles and Responsibilities

Role	Illustrative responsibility
Asset Steward	Owns the policy and the master asset inventory, and coordinates the reconciliation cycle.
Asset Owner	Maintains the classification, location, and status of an assigned asset and approves its disposition.
Procurement Reviewer	Confirms new assets are approved and registered before they enter use.
System Administrator	Applies the baseline to new assets and records the configuration.
Security Operations	Runs discovery and flags unmanaged assets for remediation.
Trust Center Coordinator	Maintains the fictional label on shared copies.

The following RACI is illustrative.

Illustrative RACI for asset lifecycle:

Activity	Asset Owner	Asset Steward	Sys Admin	Security Ops
Register a new asset	R	A	C	I
Apply the	C	I	R	I

baseline				
Run discovery	I	I	C	R
Reconcile the inventory	C	R	I	C
Approve disposition	R	A	C	I

5. Policy Requirements and Controls

PTT-POL-006-C01. Assign identifiers and owners

Every asset carries a unique identifier and a named owner. The identifier is what lets a scan result, a patch ticket, and an incident record all point at the same object, and the owner is who answers for it. A report lists any asset without an owner.

PTT-POL-006-C02. Record purpose and classification

Each asset's business use and data classification are documented so that the handling and protection rules from the classification policy can be applied without guessing. The record states what the asset is for and how sensitive it is.

PTT-POL-006-C03. Approve acquisition and assignment

New assets enter the environment only through the approved path, because an asset that arrives outside the process bypasses the baseline and the inventory at once. A new asset is approved before it enters the environment, so unplanned assets do not appear.

PTT-POL-006-C04. Apply baseline protection before use

An asset is hardened to its baseline before it handles demo data, so a freshly provisioned asset does not introduce default credentials or open services. An asset is baselined before it touches data, so it is protected from its first day.

PTT-POL-006-C05. Reconcile inventories periodically

The recorded inventory is compared to discovery results on a defined cadence, and differences are resolved so the inventory does not silently drift from reality. The reconciliation output is dated and any unknown asset is flagged.

PTT-POL-006-C06. Control transfer and disposal

Transfers update ownership and disposal follows sanitization, because an asset that leaves the environment must not carry recoverable data with it. A disposal requires a data-destruction record before the asset leaves.

PTT-POL-006-C07. Remediate unknown assets

Unmanaged or unrecognized assets are investigated and either brought under control or removed, closing the gap that discovery reveals. An unknown asset is investigated and either brought under management or removed.

PTT-POL-006-C08. Track the asset lifecycle

Each asset's stage is recorded as it moves from acquisition to disposition, so the inventory reflects current state rather than a historical snapshot. The lifecycle state is checked against the inventory each quarter.

PTT-POL-006-C09. Protect removable media

Removable media is inventoried, encrypted where it holds sensitive data, and sanitized before reuse or disposal. Removable media is tracked and its use logged, so a drive is not an unmonitored path.

PTT-POL-006-C10. Retire decommissioned assets promptly

Assets no longer in use are removed from the inventory and their data disposed, so stale assets do not accumulate as unmanaged attack surface. A decommissioned asset is removed from the inventory and its data destroyed.

PTT-POL-006-C11. Assign criticality tiers

Assets are tiered by criticality so that protection and recovery priority track importance rather than treating every asset alike. Critical assets receive the highest baseline and the shortest recovery objective. The tier assignment is reviewed when a dependency changes.

PTT-POL-006-C12. Maintain an asset relationship map

The dependencies between assets are recorded so that the blast radius of a failure or compromise is understood before it happens. The map informs recovery and containment decisions. The map is updated when a system or dependency changes.

PTT-POL-006-C13. Reconcile against procurement

The inventory is reconciled against procurement records so that an asset acquired through purchasing cannot exist outside the inventory. The inventory is checked against purchases, so a bought asset is not missing from the list.

PTT-POL-006-C14. Apply asset tagging

Assets are tagged with their environment and owner, so an asset's provenance and responsibility are visible at a glance. Tagging makes an asset visible to scanning and monitoring.

PTT-POL-006-C15. Inventory data at rest locations

The inventory records where sensitive data is stored, so the data-at-rest footprint is known and can be protected. Where data sits is recorded, so encryption and access controls cover every store.

PTT-POL-006-C16. Handle shared assets

Assets shared across teams have a single named owner, so shared ownership does not become unowned. A shared asset has a clear custodian and a defined purpose.

PTT-POL-006-C17. Flag unsupported assets

Assets approaching end of life are flagged and scheduled for replacement or compensating control, because unsupported software is the classic entry point for known vulnerabilities. An unsupported asset is listed with its planned replacement.

PTT-POL-006-C18. Record asset dependencies

The inventory notes which assets depend on which, so the impact of a failure can be understood before it happens. A dependency map turns an asset list into a basis for continuity and incident decisions. The dependency record is tested against a recovery exercise.

6. Operating Procedures

Register a new asset.

The asset owner records the identifier, purpose, and classification before the asset is used. The entry is added to the master inventory.

Apply the baseline.

The system administrator configures the asset to its security baseline and records the applied settings.

Run discovery.

Security Operations runs a discovery pass to identify assets present in the environment but not in the inventory.

Reconcile results.

Differences between discovery and inventory are resolved with the asset owner, who either registers or removes each item.

Investigate unknowns.

Unmanaged assets are traced and either onboarded under control or quarantined pending disposition.

Process transfer.

When an asset changes hands, the transfer updates ownership and the record of custody.

Sanitize at disposition.

Information-bearing media is sanitized before disposal, and the sanitization is recorded.

Update the inventory.

Every lifecycle event is reflected in the inventory so it stays current.

Tier the asset.

The asset owner assigns a criticality tier at registration, and the tier is recorded.

Map dependencies.

The relationship between the asset and its dependents is recorded in the relationship map.

Tag a new asset.

The asset is tagged with environment and owner at registration.

Record data location.

The locations where sensitive data rests are recorded in the inventory.

Onboard a new asset.

The owner records the asset in the inventory with its classification, location, and support status before it is connected to the demonstration.

Dispose of a retired asset.

The owner sanitizes the asset, records the method, and removes it from the inventory with the disposal date.

Review asset criticality.

The owner re-scores each asset's criticality and updates the tier, so the prioritization stays current.

Reconcile the inventory.

The owner compares the inventory to the actual environment, flags any unknown asset, and records the reconciliation.

Decommission an asset.

The owner records the removal, ensures data is destroyed, and updates the inventory.

Track software licenses and support dates.

The asset owner records each software license, its seat count, and its vendor support end date, so renewals and end-of-life replacements are planned before they lapse.

Reconcile cloud resources against the inventory.

The owner compares the provisioned cloud resources against the asset inventory and flags any resource that exists without a recorded owner or business justification.

Review asset ownership.

The asset manager confirms each inventoried asset has a named owner and reassigns any asset whose owner has left or changed role so no asset is unowned.

Review end-of-life assets.

The owner identifies assets approaching end of support or end of life and records a replacement or decommissioning plan before support lapses.

7. Frequency and SLAs

Illustrative asset cadence:

Activity	Frequency (illustrative)
Inventory reconciliation	Quarterly
Discovery scan	Monthly
Baseline review	Annually
Removable media check	Quarterly

8. Exceptions and Lifecycle

An exception may allow a short grace period to register a newly discovered asset when the Asset Steward documents the gap and adds interim monitoring. The exception names the asset and the date it will be brought under control.

Exceptions are reviewed quarterly and expire automatically unless renewed. An asset that remains unmanaged across two review cycles is treated as a finding and escalated rather than waived again.

An asset that remains unmanaged across two review cycles is escalated as a finding rather than waived again, because a persistent gap in the inventory is a structural problem, not a one-off oversight.

9. Records and Evidence

Record type	What it demonstrates (illustrative)
Asset inventory export	The authoritative list of identifiers, owners, and classifications.
Assignment records	The ownership and custody history.
Reconciliation report	The comparison of inventory to discovery.
Baseline application records	The applied configuration per asset.
Disposal records	Sanitization and disposition evidence.
Exception approvals	Documented grace periods.
Criticality assignments	The tier recorded per asset.
Relationship map	The documented asset dependencies.
Inventory reconciliation report	The result of the periodic inventory check.
Disposal certificates	The record of sanitization and disposal.
Asset inventory	The maintained list of assets, owners, and classifications.
Reconciliation records	The dated results of inventory reconciliations.
SBOM records	The component inventories per software asset.
End-of-life list	The assets past or near support.
License inventory	Lists each software license with its seat count, cost center, and support end date.
Cloud reconciliation report	Compares cloud resource usage against the inventory and flags unrecorded assets.
Ownership review record	Shows each asset, its owner, and any ownership change.

10. Oversight and Metrics

- Inventory coverage: 100 percent of discovered assets present in the inventory (illustrative).
- Unmanaged asset count: trending down to zero.
- Reconciliation completion: 100 percent of due reconciliations completed.
- Disposal timeliness: decommissioned assets removed within the illustrative window.
- Critical asset coverage: 100 percent of critical assets inventoried and baselined.
- Inventory accuracy: the share of sampled assets found in the inventory trending to 100 percent.
- Unsupported asset count: assets past end of life trending toward zero.
- Percentage of assets with an owner and a classification.
- Number of unknown assets discovered and remediated per period.
- Percentage of assets with an owner and classification.
- Unknown assets discovered per period.
- Assets past end-of-life.
- Inventory reconciliation errors.

11. Appendix

Illustrative asset classes:

Class	Examples (illustrative)	Owner
Endpoint	Workstations, mobile	Asset Owner
Server	Application and database hosts	Platform Team
Cloud resource	Storage, compute, managed services	Platform Team
Removable media	Drives, portable storage	Asset Steward

12. Related Policy Dependencies

- Data Classification and Handling Policy (classifies the data assets hold)
- Secure Configuration Policy (defines the baseline assets must meet)
- Patch Management Policy (uses the inventory to know what to patch)
- Vulnerability Management Policy (uses the inventory to know what to scan)
- Records Retention and Deletion Policy (governs the records this policy creates)
- Business Continuity and Disaster Recovery Policy (uses the inventory to plan recovery)

13. Review Cadence

The Asset Steward reviews this policy at least annually, after a material change to the illustrated environment, and after a significant simulated discovery gap.

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-006
Document Owner	Asset Steward
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