

PAPER TIGER TECHNOLOGIES

Acceptable Use Policy

1. Purpose

The purpose of this Acceptable Use Policy is to set the boundaries for how the fictional workforce uses systems, accounts, devices, and data in the PaperTiger demonstration. It defines what is permitted and what is prohibited so that use of the illustrated environment stays consistent with security, confidentiality, and the non-production nature of the exercise.

Acceptable-use rules matter because most security incidents begin with a person doing something outside the expected pattern. Stating the pattern in advance makes the expectation enforceable and makes a later violation attributable. A policy that is silent on acceptable use gives people no standard to follow and no basis for a consistent consequence.

This policy is fictional and illustrative. Paper Tiger Technologies is not a real company, and nothing here describes a real user, device, or enforcement action.

The policy is intentionally readable in one sitting because it is the rule set every participant is expected to internalize. Its brevity is a feature: the more people can recall the boundaries without looking them up, the more the boundaries actually govern behavior.

The rules are layered deliberately: a purpose boundary, a credential rule, a data rule, and a reporting rule. Each layer catches what the others miss, so the acceptable-use expectation holds even when one rule is unclear in a specific situation.

2. Definitions

Term	Definition (illustrative)
System	Any illustrated application, service, account, or endpoint used for demo work.
Workforce member	A fictional participant, employee, or contractor with access to the environment.
Personal use	Activity unrelated to the fictional PaperTiger service, such as private messaging or storage.
Misuse	Use of a system outside this policy, whether negligent or deliberate.
Credential	A password, token, or second factor that authenticates a workforce member.
Consequence model	The illustrative set of responses applied to confirmed violations.
Synthetic data	Clearly fictional records used in place of real

	personal or customer information.
Non-production boundary	The rule that no artifact is presented as a real policy, certificate, or commitment.
Report	A notice of suspected misuse submitted to the Information Security Lead.
Authorized tool	A tool listed in the environment guide as approved for demo work.
Reporting channel	The accessible, non-retaliatory route for reporting misuse.
Systemic cause	A training or control gap that explains repeated violations.
Shadow IT	Any application, service, or device used for demo work that was not provisioned through the approved change and access path.
Incidental use	Brief, non-commercial personal activity that does not touch synthetic customer data and does not interfere with the demonstration.
Removable media	Portable storage such as a USB drive or memory card that can be attached to a demo device and copy data off of it.

3. Scope and Boundaries

This policy applies to all fictional personnel, contractors, and anyone given access to the illustrated environment, and to company and personal devices used for demo work. It covers accounts, systems, data, and any device that touches the illustrated service boundary.

It applies regardless of whether the activity appears in a document, a simulated workflow, or an illustrative system diagram, and it applies to both intended and incidental use of the environment.

Out of scope are personal accounts and devices that have no connection to the demonstration. This policy does not govern real people, real systems, or real data, and it creates no real disciplinary or legal obligation.

The policy covers incidental use as well as deliberate use, so a participant who wanders outside the boundary by accident is still within scope for review even if the consequence differs from a deliberate act.

4. Roles and Responsibilities

Role	Illustrative responsibility
Workforce Member	Uses systems within the stated boundaries and reports suspected misuse.
Information Security Lead	Interprets the policy, investigates reported violations, and records findings.

People Lead	Applies the fictional consequence model to confirmed violations.
Access Administrator	Suspends access when a violation requires it.
Trust Center Coordinator	Confirms shared copies keep the fictional demo label.
Governance Forum	Reviews repeat or material violations as a demonstration of escalation.

5. Policy Requirements and Controls

PTT-POL-002-C01. Use systems for the intended demo purpose

Access is limited to the illustrated service work, and unrelated personal or commercial activity is out of scope. A clear purpose boundary reduces the surface where misuse can hide and makes the environment easier to monitor and review. The environment guide is versioned, and a quarterly walk of active usage is checked against it.

PTT-POL-002-C02. Protect credentials

Passwords and tokens are not shared, reused across systems, or written into shared documents. Shared credentials destroy the attribution that every other control relies on, so this is treated as a first-order rule. Credential exposure is tested with a quarterly review of where secrets are stored.

PTT-POL-002-C03. Do not introduce unauthorized material

No software, file, or configuration is added outside the approved change path, because unsanctioned additions bypass review and baseline controls. This includes downloads from personal storage.

PTT-POL-002-C04. Keep data minimal and synthetic

Only clearly fictional records are used, and real personal information is never introduced. This preserves the non-production nature of the exercise and prevents real data from contaminating a controlled demo.

PTT-POL-002-C05. Report suspected misuse

Observed policy violations are reported to the Information Security Lead without delay, because unreported misuse becomes normalized. Reporting is expected even when the observer is unsure whether a rule was broken. The reporting channel is measured by how many reports open within a day of receipt.

PTT-POL-002-C06. Respect the non-production boundary

No artifact is presented as a real policy, certificate, or operating commitment, which keeps the demonstration from being mistaken for reality. The boundary applies to external communications and shared files alike. A sample of exported artifacts is checked each month for the fictional label.

PTT-POL-002-C07. Separate demo and personal accounts

Demo work stays in demo accounts and is not mixed with personal credentials or storage, so a personal compromise cannot reach the illustrated environment. Personal devices are used only through the approved access path.

PTT-POL-002-C08. Use approved tooling

Work is performed with the tools listed in the environment guide, which keeps the toolset within the reviewed and patched boundary. New tools enter only through the change process. The tool list is reconciled against actual usage each quarter.

PTT-POL-002-C09. Avoid deceptive content

No participant fabricates customer, vendor, or certification claims, even within the demo, because deceptive content undermines the exercise and could be mistaken for a real assertion. A fabricated claim is corrected and its source reviewed, because deceptive content undermines the exercise.

PTT-POL-002-C10. Follow acceptable network use

Network access is used for the demo purpose only, and scanning or probing outside the illustrated boundary is not permitted. Any security testing is confined to the authorized scope.

PTT-POL-002-C11. Apply the consequence model consistently

Confirmed violations receive a consequence proportionate to intent and impact, and similar violations receive similar treatment. Consistency is what makes the policy credible rather than arbitrary. Consequence decisions are reviewed quarterly for proportionality.

PTT-POL-002-C12. Review violations for systemic cause

Repeat violations are examined for whether they trace to a training gap or a control weakness rather than an isolated individual, so the program fixes the cause rather than only the symptom.

PTT-POL-002-C13. Protect the reporting channel

The reporting channel is accessible and non-retaliatory, so participants are willing to report rather than staying silent. A report made in good faith is treated as cooperation.

PTT-POL-002-C14. Govern personal device use

Personal devices used for demo work are subject to the same access and data rules as company devices, so a personal device does not become a bypass around the boundary. A check confirms no demo credential is stored on a personal device.

PTT-POL-002-C15. Restrict external storage

External storage and file-sharing outside the approved toolset are restricted, so data does not leave the environment through an unapproved channel. The approved storage list is re-verified on a schedule.

PTT-POL-002-C16. Set expectations for public statements

Public statements about the demonstration remain within the fictional framing, so a participant does not present the demo as a real company or product.

PTT-POL-002-C17. Apply the policy to contractors

Contractors are held to the same acceptable-use rules as employees, so a third party does not operate under a looser standard.

PTT-POL-002-C18. Bound incidental personal use

Brief personal use is permitted only when it is unrelated to the demo, does not touch synthetic data, and does not consume meaningful resources. The boundary exists because a total prohibition is unrealistic and unenforceable, while an open allowance would let personal activity contaminate the controlled environment. Incidental use must not interfere with the demo purpose or consume shared resources.

PTT-POL-002-C19. Prohibit resale or reuse of demo assets

No participant repurposes illustrated systems, data, or outputs for personal gain or outside the demonstration. This keeps the fictional boundary intact and prevents demo artifacts from being mistaken for real products or services. A demo asset is used only for the exercise, and reuse outside it is treated as a violation.

PTT-POL-002-C20. Control removable media

Removable media is used only through the approved path, scanned before attachment, and logged, because portable storage is the easiest way to move data outside a boundary without leaving a network trace. Removable media is tracked, and its use is limited to an approved, logged purpose.

PTT-POL-002-C21. Require prompt loss reporting

A lost or stolen device or credential is reported to the Information Security Lead immediately, because a silent loss leaves an account exposed with no one looking. Prompt reporting triggers

suspension and review before misuse can compound. A lost device is reported immediately, and the associated credentials are revoked without waiting.

PTT-POL-002-C22. Prohibit tampering with monitoring

Participants do not disable, bypass, or alter logging and monitoring that is active on the environment, because the acceptable-use rules depend on a record of what actually happened. Disabling monitoring is itself treated as a violation.

6. Operating Procedures

Acknowledge the policy.

Each participant records acceptance before first access to the illustrated environment, and the acceptance is retained as evidence of the boundary being communicated.

Request access through the access process.

Accounts are provisioned only through the Identity and Authentication Policy path, never created ad hoc, so every account has an approval behind it.

Use approved tooling.

Work is performed with the tools and accounts listed in the environment guide, and any exception is requested rather than assumed.

Report a concern.

The reporter describes the issue and preserves relevant records for review, without investigating on their own or alerting the subject.

Investigate.

The Information Security Lead gathers context, interviews the relevant parties, and determines whether a violation occurred and its severity.

Apply the consequence.

The People Lead applies the fictional consequence model appropriate to the confirmed violation, proportionate to intent and impact.

Record the outcome.

Findings and any illustrative consequence are logged in the demo incident or case register for trend review.

Review for trends.

Repeat violations are reviewed for patterns that indicate a gap in training or a control rather than an isolated individual.

Suspend on serious misuse.

The Access Administrator suspends access when a violation requires it, and the suspension is recorded with the reason.

Remediate a training gap.

A pattern of violations triggers a targeted awareness refresh rather than a repeat of the same consequence.

Enroll a personal device.

A personal device used for demo work is enrolled under the access rules and its use is recorded.

Review external storage use.

External storage and sharing are reviewed for adherence to the approved toolset.

Handle a lost or stolen device.

The reporter notifies the Information Security Lead, the Access Administrator suspends the affected accounts, and the event is recorded in the incident register with a description of what may have been exposed.

Review an incidental-use request.

A participant requests a specific incidental use, the Information Security Lead confirms it stays within the boundary, and the approval is logged with its duration and any compensating condition.

Review a new tool request.

The requester describes the tool and purpose, the owner checks it against the approved list, and the decision is recorded.

Handle a lost device.

The participant reports the loss immediately, the owner revokes the associated credentials, and the incident is logged.

7. Frequency and SLAs

Illustrative enforcement cadence:

Activity	Frequency (illustrative)
----------	--------------------------

Acceptance record	Before first access
Violation investigation	As reported
Trend review	Quarterly
Policy review	Annually

8. Exceptions and Lifecycle

An exception may permit a one-off use not otherwise allowed, such as a controlled integration test, when the Information Security Lead documents the specific use, its duration, and any compensating controls. The request names the account, the purpose, and the expected end.

Exceptions are time-boxed and reviewed at least quarterly. An exception that recurs becomes a candidate for a policy change rather than a repeated waiver, and any exception that touches data or external access requires an additional compensating control.

A recurring exception, such as a repeated one-off integration test, becomes a candidate for a policy change rather than a repeated waiver, and the change is routed through the normal review.

9. Records and Evidence

Record type	What it demonstrates (illustrative)
Signed acceptance records	Confirmation each participant accepted the policy before access.
Access request approvals	The approved provisioning path for each account.
Reported-concern log	The intake of reported misuse.
Investigation notes	The gathered context and determination.
Consequence records	The applied fictional consequence.
Exception approvals	Documented one-off uses.
Consequence register	The applied responses with proportionality notes.
Trend review	The quarterly look at repeat violations.
Device loss report	The record of a lost or stolen device and the suspension action taken.
Removable media log	The register of media attached, scanned, and removed.
Incidental-use approvals	The logged approvals and their durations.
Tool approval log	The dated decisions on tool requests.
Violation reports	The recorded reports and their dispositions.

10. Oversight and Metrics

- Acceptance completion: 100 percent of active participants recorded acceptance (illustrative).

- Reported misuse: reports triaged within one business day in the demo.
- Repeat violations: trending down quarter over quarter.
- Exception count: open exceptions flat or declining.
- Reporting accessibility: the reporting channel available and known to all participants.
- Incidental-use exception rate: the number of approved incidental uses trending flat or down.
- Lost device time-to-report: median time between loss and report within one business day.
- Violations by category per period.
- Time from loss report to credential revocation.

11. Appendix

Illustrative prohibited activities:

Activity	Illustrative handling
Sharing credentials	Investigation and consequence
Introducing real personal data	Immediate removal and review
Unauthorized software	Removal and change-path correction
Presenting demo as real	Correction and boundary reinforcement

12. Related Policy Dependencies

- Identity and Authentication Policy (governs the accounts this policy constrains)
- Security Access Policy (defines access to customer environments)
- Data Classification and Handling Policy (governs the data this policy protects)
- Incident Response Policy (handles misuse that escalates to an incident)
- Security Awareness and Training Policy (feeds the gaps this policy reveals)

13. Review Cadence

The Information Security Lead reviews this policy at least annually, after a material change to the illustrated environment, and after a significant simulated violation.

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-002
Document Owner	Information Security 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