

PAPER TIGER TECHNOLOGIES

Information Request Policy Statement

1. Purpose

The purpose of this Information Request Policy Statement is to describe how Paper Tiger would respond to requests for data from government agencies or other parties. It distinguishes customer data from Paper Tiger business records and preserves notification.

When a third party asks a service provider for data, the provider must know whose data it is and who is best positioned to respond. This statement sets out that reasoning so that customer data is referred to the customer and only Paper Tiger's own records are reviewed against legal process.

This statement is fictional and illustrative. It describes no real request, agency, or disclosure.

The statement distinguishes customer data from business records because the whole response depends on whose data it is, and referring customer data to the customer is both correct and protective.

The statement exists so a trust review can see how the organization would answer a request, and the policy makes that answer prompt, verified, and safely bounded.

The statement exists so a customer knows what the provider will share and how quickly, and the policy turns that posture into a process with verification, scoping, and a record.

2. Definitions

Term	Definition (illustrative)
Request	A demand for data from a government agency or other party.
Customer data	The vendor records a customer owns and controls.
Business records	Paper Tiger's own account, billing, and operational records.
Legal process	A subpoena, court order, warrant, or equivalent instrument.
Notification	The notice to a customer before their data is disclosed.
Referral	Directing a requester to the customer as controller.
Challenge	The act of resisting an overbroad or defective

	request.
Mutual legal assistance	A recognized channel for cross-border requests.
Letter rogatory	A formal request from one court to another.
Proportionality	The principle that a request's scope matches its need.
Request lifecycle	The stages from receipt to disposition.
Legal coordination	The review of responses with legal counsel.
Preservation	The retention of data during a dispute.
Information request	A request from a customer or regulator for information about the platform's security, privacy, or handling practices.
Response window	The stated time within which a request is acknowledged and answered.
Business record	A document that describes the illustrated organization's own operations, as distinct from customer data.
Out-of-scope data	Material that belongs to other customers or to internal operations and is excluded from a given response.
Response standard	The committed turnaround and format for answering a request.
Requester verification	The confirmation that a request comes from an authorized contact.
Request log	The maintained record of requests and their dispositions.
Subpoena	A legal demand for records or testimony.
Gag order	A restriction on disclosing that a request was received.
Disclosure	The release of data in response to a request.
Confidentiality	The protection of data from unauthorized disclosure.
Acknowledgment	The confirmation of receipt and timeline.
Dispute preservation	The holding of data while a request is challenged.
International request	A request with a cross-border element.
Over-broad request	A request that exceeds its lawful scope.
Narrowing	The reduction of a request to its lawful scope.
Response template	A standard document structure used to answer a recurring request type consistently.
Request SLA	The maximum time allowed to respond to a given request type.
Request routing	The process of directing a request to the parties that hold relevant data.

3. Scope and Boundaries

This statement applies to fictional requests directed at customer data or Paper Tiger business records in the illustrated service. It covers both domestic and international requests.

It applies to any request regardless of the form in which it arrives, so a request is treated the same whether it is a formal instrument or an informal inquiry.

Out of scope are real requests and real data. This statement creates no real legal obligation.

The scope includes informal inquiries as well as formal instruments, so a request is classified the same whether it arrives as a warrant or as a question.

Escalation for an unclear request follows a fixed chain: the responder flags the ask, the Information Security Lead decides whether it is answerable, and the governance forum resolves any request that touches legal or contractual interpretation.

The statement covers requests about the provider's handling of customer data; requests for a customer's own records are the customer's to answer.

The statement is a fictional demonstration of a request-handling posture; it does not bind the provider to any real response commitment.

The statement is reviewed when the underlying policies change, so it does not describe a posture that the rest of the library no longer holds.

The statement is reviewed whenever the underlying data-handling policies change, so it stays aligned with the rest of the library.

This policy applies to requests from data subjects, regulators, and law enforcement, whether received directly or through a customer.

4. Roles and Responsibilities

Role	Illustrative responsibility
Legal and Privacy Lead	Owns the statement and reviews requests.
Customer	Owns and controls customer data and is the primary responder.
Security Operations	Supports preservation and review when a valid process arrives.
Trust Center Coordinator	Maintains the fictional label on shared copies.

The following RACI is illustrative.

Illustrative RACI for request handling:

Activity	Legal and Privacy	Customer	Security Ops
----------	-------------------	----------	--------------

	Lead		
Receive and classify	R	I	C
Validate the instrument	R	I	C
Refer customer data	R	A	I
Notify	R	I	I
Challenge	R	C	I

5. Policy Requirements and Controls

PTT-POL-022-C01. Distinguish data types

Requests are sorted into customer data versus Paper Tiger business records, because the response path depends entirely on who controls the data. Misclassifying data would send the wrong party the wrong instruction. The data type is recorded before the response.

PTT-POL-022-C02. Require valid legal process

Paper Tiger responds only to a lawful instrument such as a subpoena, order, or warrant. A request without a valid instrument is not acted on, which protects both the customer and the provider. A request needs valid process, so the provider does not hand data over casually.

PTT-POL-022-C03. Direct customer-data requests to the customer

Requests for customer data are referred to the customer as controller, because the customer is the party best positioned to respond and to assert any objection. A customer-data request is directed to the customer.

PTT-POL-022-C04. Notify before disclosure

The customer is notified before their data is disclosed unless prohibited, so the customer can seek relief before any production occurs. The customer is notified before disclosure where allowed.

PTT-POL-022-C05. Review for scope and validity

Each request is checked for facial validity, scope, and proportionality, so an overbroad request is narrowed rather than accepted at face value. The scope check is dated.

PTT-POL-022-C06. Resist or challenge where appropriate

Requests are challenged when they are overbroad or defective, so the provider does not become a passive conduit for an improper demand. An over-broad request is challenged.

PTT-POL-022-C07. Handle international requests through channels

Foreign requests are evaluated through mutual legal assistance or letters rogatory, so cross-border demands follow a recognized path. An international request goes through the right channel.

PTT-POL-022-C08. Preserve the non-production boundary

This statement is illustrative and is not presented as a real legal position or commitment. The fictional boundary is preserved in every response.

PTT-POL-022-C09. Log the request lifecycle

Each request is logged from receipt through disposition, so the handling of any request can be reconstructed. Each state change is logged.

PTT-POL-022-C10. Coordinate with legal

Requests are coordinated with the legal and privacy lead, so the provider's response is consistent and defensible. Legal review is recorded for sensitive requests.

PTT-POL-022-C11. Preserve during dispute

Data that is the subject of a dispute is preserved, so a challenge does not destroy the very data at issue. Data is preserved while a request is disputed.

PTT-POL-022-C12. Document the response rationale

Each response decision is documented with its rationale, so the handling is defensible. The rationale for the response is recorded.

PTT-POL-022-C13. Coordinate with subprocessors

Requests that may involve a subprocessor are coordinated, so the provider does not respond on behalf of a party it does not control. A subprocessor is coordinated with when it holds the data.

PTT-POL-022-C14. Review the statement

The statement is reviewed periodically and after a significant request, so it stays current.

PTT-POL-022-C15. Route requests to a single owner

All information requests are received and tracked by a named owner, so a request does not fall between teams or get answered inconsistently. A single owner handles the request, so it is not dropped.

PTT-POL-022-C16. Acknowledge within the window

Each request is acknowledged within a short, stated window so the requester knows it was received and is being handled.

PTT-POL-022-C17. Verify the requester

A request for information is verified to be from who it claims, so the organization does not hand sensitive detail to the wrong party. The verification is recorded before release.

PTT-POL-022-C18. Answer only what was asked

The response covers the request without volunteering unrelated detail, because over-sharing in a trust context is itself a disclosure risk. The response is checked against the request scope.

PTT-POL-022-C19. Redact other customers' material

Anything outside the request's scope is removed before delivery, so no response becomes an accidental disclosure of another party's information. Out-of-scope material is redacted.

PTT-POL-022-C20. Set a response timeline

The provider commits to a defined turnaround and tells the requester when the ask is larger than the standard window, so expectations are set before work begins. The timeline is told to the requester and met.

PTT-POL-022-C21. Escalate unclear asks

A request that is ambiguous or unusually broad goes to the Information Security Lead before it is answered, so a mistake is caught early. An unclear request is escalated before it is answered.

PTT-POL-022-C22. Offer a standard format

Responses follow a consistent structure, so the requester can read the answer without a custom explanation each time. The response follows a standard format.

PTT-POL-022-C23. Protect the requester's information

The identity and context of a requester are handled as confidential, so a request does not become its own disclosure. The requester's identity is held confidential.

6. Operating Procedures

Receive and classify.

The request is logged and classified by data type.

Validate the instrument.

The request is checked for a lawful, scoped instrument.

Refer or review.

Customer-data requests are referred; business-record requests are reviewed.

Notify the customer.

Notification is sent before any disclosure.

Challenge if defective.

Overbroad or defective requests are resisted.

Record the outcome.

The decision and any production are logged.

Log the request.

The request is logged with its classification and the instrument provided.

Coordinate the response.

The legal and privacy lead reviews the response before it is sent.

Document a response.

The response decision and its rationale are recorded.

Coordinate with subprocessors.

A request involving a subprocessor is coordinated before response.

Log an incoming request.

The request is recorded with its source, subject, and date, and an owner is assigned.

Draft and review a response.

The owner drafts the response, a reviewer confirms accuracy and the disclosure, and the response is sent and logged.

Validate a request.

The responder confirms the requester's authorization and the named scope before any data is collected for the response.

Redact before delivery.

The responder removes out-of-scope material, marks the response with the fictional disclosure, and has a second person review before sending.

Close and record a request.

The responder records the disposition and any follow-up, then files the request and response in the tracking log.

Assemble a response.

The responder gathers only the in-scope data, applies the fictional disclosure, and has a reviewer confirm before delivery.

Review request trends.

The responder summarizes the requests by type, and the Information Security Lead uses the trend to improve the standing documentation.

Challenge an over-broad request.

The responder documents the objection, legal reviews it, and the narrowed scope is negotiated.

Coordinate with a subprocessor.

The responder contacts the subprocessor that holds the data and confirms what it can produce.

Acknowledge a request.

The responder confirms receipt and sets the expected timeline with the requester.

Draft a response.

The responder gathers in-scope data and applies the fictional disclosure before review.

Preserve during dispute.

The provider holds the relevant data while the request is challenged.

Handle an international request.

The responder routes the request through the right channel and coordinates with legal.

Coordinate with legal.

Legal reviews a sensitive request before a response is drafted.

Resist an over-broad request.

The responder documents the objection, legal reviews it, and the scope is narrowed.

Maintain a response template.

The request team keeps a standard response template for each request type so answers are consistent and complete without starting from scratch each time.

Track the request SLA.

The team records each request's receipt date and due date and reviews overdue items so deadlines are not missed.

Coordinate with subprocessors on requests.

The request team notifies any subprocessor that holds relevant data and directs it to support the response within the same deadline, so nothing is missed.

7. Frequency and SLAs

Illustrative request cadence:

Activity	Frequency (illustrative)
Request classification	On receipt
Notification	Before disclosure
Challenge decision	As applicable
Statement review	Annually

8. Exceptions and Lifecycle

An exception permits shortening or skipping notification when a court order specifically prohibits it and the Legal and Privacy Lead documents the basis.

Exceptions are reviewed after the matter closes, and a notification exception is the highest-scrutiny case.

A notification exception is the highest-scrutiny case and is reviewed after the matter closes, because skipping notification is the single most consequential deviation this statement allows.

9. Records and Evidence

Record type	What it demonstrates (illustrative)
Request log	The received requests.
Classification records	The data-type determinations.
Validity review notes	The instrument checks.
Notification records	The customer notifications.
Challenge records	The resisted requests.
Request lifecycle log	The reconstructed handling.
Response coordination	The legal review of responses.
Response records	The issued responses and their reviews.
Response copy	The redacted response as delivered, kept for audit.
Response copies	The redacted responses as delivered, kept for audit.

Legal review records	The dated legal reviews of requests.
Disclosure log	The recorded disclosures and their basis.
Response template	The standard document used to answer each recurring request type.
SLA compliance report	Shows each request's receipt and response date against its deadline.
Request routing log	Shows each request and the parties engaged to support it.

10. Oversight and Metrics

- Classification accuracy: 100 percent of requests correctly classified (illustrative).
- Notification: sent before every disclosure not prohibited.
- Invalid requests: not acted on.
- Challenge rate: overbroad requests challenged where appropriate.
- Classification accuracy: 100 percent of requests correctly classified.
- Response time: the median time from request to response within the stated window.
- Request backlog: the count of unanswered requests past due trending toward zero.
- Percentage of requests answered within the committed window
- Number of requests escalated for review each month
- Percentage of requests answered within the window.
- Requests escalated for review each month.
- Requests challenged or narrowed per period.
- Time from request to legal review.
- Challenges upheld.
- Disclosures reviewed by legal.

11. Appendix

Illustrative request handling:

Request type	Illustrative response
Customer data	Refer to the customer (controller)
Paper Tiger business records	Review against valid legal process
Foreign request	Evaluate via MLAT or letter rogatory

12. Related Policy Dependencies

- Data Processing Addendum (defines the controller-processor roles)
- Privacy Policy (governs the personal data at issue)
- Subprocessor List (discloses who may hold the data)
- Incident Response Policy (coordinates with legal process during an incident)

13. Review Cadence

The Legal and Privacy Lead reviews this statement at least annually, after a significant simulated request, and after a change to the illustrated legal framework.

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-022
Document Owner	Legal and Privacy 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