

PAPER TIGER TECHNOLOGIES

Security Access Policy

1. Purpose

The purpose of this Security Access Policy is to define how Paper Tiger approaches access to a customer's use of the PaperTiger platform. It describes the teams that may access the environment, the approval model customers control, and the data and systems the access arrangements cover.

Access is the point where a service provider's personnel and a customer's data meet, so the terms of that access must be explicit and customer-controlled. This policy makes the default conservative and puts the customer in charge of who may touch their instance, which is what allows a customer to accept a SaaS relationship with confidence.

This policy is fictional and illustrative. It describes no real customer, system, or access event, and it is not an operating commitment or certification.

The access model is deliberately graduated because customers differ in their risk appetite, and a single one-size-fits-all access level would either over-expose cautious customers or over-burden permissive ones. Giving the customer the choice makes the model a product of their risk decision.

The access model is a product of the customer's risk decision, and giving the customer the choice of full, incident-to-incident, or no-authorization access is what makes the model workable across customers with very different appetites.

Access to customer environments is the single most sensitive capability Paper Tiger holds, so the policy ties every grant to an authorization and removes it the moment the need ends.

Access control exists so a person holds only the access their task requires, and the policy makes every grant authorized, scoped, and reviewed.

2. Definitions

Term	Definition (illustrative)
Customer instance	The illustrated separation of a customer's data and configuration within the platform.
Authorized approver	A person the customer names who may approve access to their instance.
Security team	The fictional group that governs access and monitors posture.

Platform team	The fictional group that performs maintenance and upgrades.
Full access	Pre-approved access to the systems needed for support without per-incident approval.
Incident-to-incident	Access that requires approval each time an issue occurs.
No authorization	No access to customer systems; issues are resolved with the customer present.
Access event	A recorded grant, use, or revocation of access.
Standing access	Access that persists beyond a single task or incident.
Response time	The illustrative time to begin work on a support issue.
Governance access	The access used to review and audit other access.
Access history	The retained record of grants, approvals, and revocations.
Objection	A customer's documented concern about access.
Customer environment	The illustrated set of systems, data, and configuration that a fictional PaperTiger customer operates, which Paper Tiger accesses only with explicit authorization.
Break-glass access	An emergency access path used only when the normal approval path is unavailable and the customer cannot be reached in time.
Segregation of duties	The separation of responsibilities so that no single participant can both request and approve a material access change.
Graduated authorization	Access levels that scale with the sensitivity of the data.
Approver	The role that authorizes a data-access request.
Graduated model	The tiered access levels by sensitivity.

3. Scope and Boundaries

This policy applies to the fictional customer portal, the scoring pipeline, and the supporting infrastructure that maintain them in the demonstration. It covers the security and platform teams and any other role that could access a customer instance.

It applies to both customer data and the systems that hold it, and to standing and per-incident access alike, so that no access path is left outside the approval model.

Out of scope are any real customer environments, systems, or data. This policy authorizes nothing in the real world and is not a statement of real operational access.

The scope includes standing and per-incident access alike, so no access path sits outside the approval model, and any role that could reach a customer instance is governed whether it is a human or a service.

Access is reviewed against current need on a schedule, and a mismatch is corrected or becomes a documented exception.

4. Roles and Responsibilities

Role	Illustrative responsibility
Security Team	Approves access, monitors posture, and does not touch customer data without authorization.
Platform Team	Performs maintenance and upgrades within the approved access scope.
Customer Authorized Approver	Approves access requests for the customer's instance.
Platform Security Lead	Owns the policy and the access model.
Support Coordinator	Routes incidents and tracks the authorization type.
Trust Center Coordinator	Keeps this policy labeled as a fictional artifact.

The following RACI is illustrative.

Illustrative RACI for access decisions:

Activity	Customer Approver	Security Team	Platform Team	Support Coordinator
Name authorized approvers	A	I	I	I
Approve access request	A	C	I	R
Perform maintenance	I	I	R	C
Log access events	I	R	R	C
Review standing access	C	R	I	I

5. Policy Requirements and Controls

PTT-POL-003-C01. Limit the number of authorized approvers

A customer names up to five authorized approvers who can approve access to their instance. A bounded list prevents approval authority from becoming diffuse and hard to audit, and it keeps the customer aware of exactly who holds that authority. The approver list is reviewed quarterly and a departed approver is removed the same day.

PTT-POL-003-C02. Separate security and maintenance duties

The security team governs access while the platform team performs scoped maintenance, so the party that approves is not the party that acts. This separation prevents a single team from both granting itself access and then using it. A periodic check confirms no role both requests and approves its own access.

PTT-POL-003-C03. Require authorization before data access

Neither team accesses customer data without a documented, approved reason, because unapproved data access is the single highest-risk event this policy exists to prevent. The reason is recorded before the access occurs. A sample of access events is matched to its authorization each month.

PTT-POL-003-C04. Offer graduated authorization models

Customers choose full, incident-to-incident, or no-authorization access for their systems, matching the access level to the customer's risk appetite. The choice is respected for every subsequent request. The model is chosen to match the sensitivity of the data, so low-risk access is not over-governed.

PTT-POL-003-C05. Log every access event

Access and approvals are recorded so the decision and actor are traceable after the fact. The log captures who, what system, what reason, and for what window. The log is sampled for completeness and the sample result is recorded.

PTT-POL-003-C06. Reconfirm access reviews

Approver lists and standing access are reviewed on a defined cadence so that stale approvals do not persist and former approvers do not retain authority. The review is dated, and a missed review is escalated.

PTT-POL-003-C07. Hold the non-production label

This access model is illustrative and is never presented as a real operational commitment or certification, keeping the demonstration boundary intact. The label is preserved on every copy and never stripped to make a demo look real.

PTT-POL-003-C08. Scope access to the task

Each grant covers only the system and time window the task requires, minimizing the surface exposed during support and preventing access from drifting beyond its purpose. Over-broad requests are counted and reviewed for a systemic cause.

PTT-POL-003-C09. Require authentication for access

Every access path uses the authentication required by the Identity and Authentication Policy, so access is tied to a verified identity. Authentication precedes every access event, and an unauthenticated attempt is flagged.

PTT-POL-003-C10. Notify on access

The customer is made aware of access that touches their data, within the constraints of the incident process, so access is never silent.

PTT-POL-003-C11. Separate support from governance access

The support function operates under the customer's authorization model while the governance function reviews and audits that access, so the party being reviewed is not the party doing the reviewing.

PTT-POL-003-C12. Retain access history

The history of grants, approvals, and revocations is retained for the illustrative period so that past access can be reconstructed during a review or dispute.

PTT-POL-003-C13. Handle customer objections

A customer objection to access is escalated and resolved before further access proceeds, and the resolution is recorded so the customer's concern is not overridden silently.

PTT-POL-003-C14. Document the support model

The support model that accompanies each authorization type is documented, so a customer knows what response to expect under each choice.

PTT-POL-003-C15. Segregate customer instances

Customer instances are logically segregated so that access to one does not imply access to another, protecting isolation between customers.

PTT-POL-003-C16. Apply break-glass access

A break-glass path exists for the provider but is logged and reviewed, so even emergency access is governed rather than unmanaged. Each break-glass use is reviewed within a day of the event.

PTT-POL-003-C17. Enforce least-privilege access

A participant is granted only the permissions needed for their current task, and nothing more, so a compromised or careless account can reach only a narrow slice of the environment. Privilege is reviewed whenever a role changes and removed when a task ends. New grants are sampled to confirm they started minimal.

PTT-POL-003-C18. Separate request from approval

The person who requests a change to access is not the person who approves it, so a single actor cannot silently expand their own reach. The segregation is applied to provisioning, modification, and termination alike. The requester and the approver are different people, so no one approves their own access.

PTT-POL-003-C19. Use a documented break-glass path

Emergency access is available only through a pre-authorized break-glass procedure that is logged, time-boxed, and reviewed after the fact. The path exists because a customer incident can outpace the normal approval cycle, but it is controlled so it is not a standing back door.

PTT-POL-003-C20. Review access on role change

Access is re-checked when a person's role changes, so privileges follow the current need rather than the previous job. A role change triggers a re-check of access, and privileges not needed for the new role are removed.

PTT-POL-003-C21. Audit access events on a schedule

A sample of access events is reviewed against approvals, so a mismatch is found by inspection rather than by incident. The audit sample size and frequency are documented.

6. Operating Procedures

Name the approvers.

The customer records the list of up to five authorized approvers and keeps it current as personnel change. The list is confirmed at each quarterly review.

Submit an access request.

The requester states the system, reason, and expected duration of the access. The request is logged before any access occurs.

Obtain approval.

An authorized approver approves or denies before access is granted. The decision and its timestamp are retained.

Perform the scoped task.

Work stays within the approved system and time window, and the technician does not broaden the access on their own.

Record the event.

The access, approval, and action are logged for later review and audit.

Revoke on completion.

Access is removed when the approved window closes, and the revocation is logged.

Review standing access.

Approver lists and recurring access are revalidated on schedule, and stale entries are removed.

Escalate disputes.

A customer objection to access is escalated to the Platform Security Lead and resolved before further access proceeds.

Reconcile the approver list.

The list of authorized approvers is compared against current customer contacts quarterly, and mismatches are corrected.

Audit access events.

A periodic audit samples access events against approvals to confirm no event lacked a decision.

Document the support model.

The support expectations per authorization type are recorded and shared with the customer.

Review break-glass use.

Any break-glass access is reviewed within one business day in the demo.

Run a break-glass access event.

The requester declares the emergency, the authorizing role confirms it, access is granted with a strict time limit, and the full sequence is logged and reviewed within one business day.

Re-certify a customer's access list.

The customer owner reviews the current access list, marks each permission still required or to be removed, and the removals are actioned immediately.

Record a customer authorization.

The approver records who authorized the access, for what task, and for how long.

Review access events.

A sample of access events is reviewed against approvals, and a mismatch is corrected or documented.

Reconfirm an access review.

The reviewer re-checks the access list against current need and removes any entry that no longer applies.

7. Frequency and SLAs

Illustrative access review cadence:

Activity	Frequency (illustrative)
Approver list review	Quarterly
Standing access review	Quarterly
Access event logging	Continuous
Policy review	Annually

8. Exceptions and Lifecycle

An exception permits a temporary deviation, such as emergency maintenance under incident-to-incident terms, when the Platform Security Lead documents the justification and the customer approver confirms it. Emergency access is recorded with the reason and the window.

Emergency access is reviewed within one business day in the demo. Any access that occurred without prior approval is treated as an exception and reported, and recurring emergency access triggers a review of the authorization model rather than a standing waiver.

Recurring emergency access is reviewed for whether the authorization model itself should change, because a pattern of emergency exceptions indicates the standing access level is set too low for the customer's actual needs.

9. Records and Evidence

Record type	What it demonstrates (illustrative)
Approver list	The current customer-designated approvers.
Access request records	The system, reason, and duration requested.
Approval records	The approver decision and timestamp.
Access logs	The recorded access events.
Periodic access review output	The revalidation of standing access.
Exception approvals	Emergency and deviation records.
Approver reconciliation	The quarterly comparison of approvers to

	contacts.
Access audit sample	The sampled events checked against approvals.
Customer authorization records	The authorization behind each access grant.
Break-glass logs	The logged emergency access events and their reviews.
Access re-certification records	The periodic review outcomes and removals.
Authorization records	The dated customer authorizations.
Access review results	The dated outcomes of periodic reviews.
Access review log	The dated access reviews.

10. Oversight and Metrics

- Approval timeliness: incident-to-incident approvals returned within the illustrative window.
- Unapproved access: zero access events without a documented approval.
- Access review completion: 100 percent of due reviews completed (illustrative).
- Standing access count: trending down or stable.
- Access audit: 100 percent of sampled events matched an approval.
- Orphaned account rate: accounts with no current authorization trending toward zero.
- Break-glass usage: emergency access events reviewed within one business day.
- Percentage of access events matching an approval.
- Time from role change to access update.
- Approvers re-verified on schedule.
- Access events unmatched to an approval.

11. Appendix

Illustrative authorization types and expected impact:

Authorization type	Illustrative response impact
Full access	Standard illustrative response time
Incident-to-incident	Additional time to obtain approval per incident
No authorization	Additional time and customer availability required

12. Related Policy Dependencies

- Identity and Authentication Policy (defines how access is authenticated)
- Privileged Access Policy (governs elevated access used during maintenance)
- Logging and Monitoring Policy (captures the access events this policy requires)
- Incident Response Policy (governs access during an incident)
- Secure Configuration Policy (defines the systems this access reaches)

13. Review Cadence

The Platform Security Lead reviews this policy at least annually, after a change to the illustrated access model, and after a significant simulated access event.

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-003
Document Owner	Platform 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