

PAPER TIGER TECHNOLOGIES

Privileged Access Policy

1. Purpose

The purpose of this Privileged Access Policy is to control accounts and sessions that carry elevated authority in the PaperTiger environment. Privileged access is limited, approved, logged, and reviewed so that high-impact actions remain attributable.

Privileged accounts are the highest-value target in any environment because they can change security configuration, read sensitive data, and erase evidence. Treating them separately from standard accounts is what keeps a single compromise from becoming total control, and it is why this policy exists as its own document rather than a subsection of the identity policy.

This policy is fictional and illustrative. It describes no real account, credential, or session.

The policy exists as its own document rather than a subsection of the identity policy because privileged access carries a different threat model: the attacker who reaches an administrator is not the same adversary as the one who reaches a standard user, and the controls must reflect that.

Privileged access is where a small mistake becomes a large exposure, so the policy concentrates the strongest controls, vaulting, recording, and justification, on that narrow and powerful surface.

The policy's whole aim is to shrink the privileged surface to the smallest window that still lets the work happen, and to make every use of that window loud and attributable.

Privileged access management exists to bound the damage a single account can do, and the policy makes every elevation justified, scoped, and temporary.

2. Definitions

Term	Definition (illustrative)
Privileged account	An account with rights beyond a standard user, such as administrative rights.
Just-in-time access	Elevated rights granted for a task and removed when the task ends.
Break-glass account	An emergency account used only when normal access is unavailable.
Privileged session	A login session using elevated rights.
Elevation	The act of granting or assuming elevated

	rights.
Privilege approver	The role that approves grant and elevation requests.
Standing privilege	Elevated rights that persist across tasks.
Session logging	The recording of commands and actions in a privileged session.
Credential vault	The controlled store for privileged credentials.
Least privilege	The minimum rights needed for the task.
Privilege tier	The division of privilege into scoped and full levels.
Justification	The recorded business reason for an elevation.
Vault monitoring	The logging and alerting on access to the credential store.
Session recording	The capture of a privileged session's actions so they can be reviewed after the fact.
Vaulting	The storage and rotation of privileged credentials in a controlled store so they are not distributed in the clear.
Break-glass	The emergency path to privileged access when normal approval fails.
Blast radius	The scope of damage a single compromised account could cause.
Privileged entitlement	A standing right to perform a privileged action.
Privileged access management	The system that vaults and rotates privileged credentials.
Jump server	The controlled host through which privileged access flows.
Administrator	A role with elevated control over a system.
Dormant account	A privileged account that has not been used for a set number of days and therefore no longer justifies standing access.
Dual control	A requirement that two separate people approve or perform a sensitive action so that one person cannot act alone.
Credential compromise	The suspected or confirmed loss of control of an account's credentials to an unauthorized party.

3. Scope and Boundaries

This policy applies to administrator accounts, break-glass accounts, service accounts with elevated rights, and any session capable of changing security configuration in the demo. It covers both standing and temporary privilege.

It applies to the fictional platform, its supporting infrastructure, and the tools used to administer them, so that no elevated path sits outside the approval and logging model.

Out of scope are real systems, real accounts, and real credentials. This policy creates no real access and is not an operational commitment.

Service accounts with elevated rights are in scope alongside human administrators, because a machine credential with broad rights is equally capable of changing configuration and is often less watched.

Escalation for privileged access follows a fixed chain: an unexplained elevated action goes to the privileged access administrator, then to the Information Security Lead, and finally to the governance forum when the action indicates a compromise. Each escalation and its resolution is recorded.

Privileged access is reviewed against need on a schedule and is part of the fictional demonstration.

This policy applies to human user accounts, service accounts, and third-party administrators with elevated rights, including access granted temporarily through a contractor engagement.

4. Roles and Responsibilities

Role	Illustrative responsibility
Privileged Access Lead	Owns the policy and the privileged account inventory.
Privilege Approver	Approves grant and elevation requests.
Privileged User	Uses elevated rights only for the approved task.
Vault Custodian	Operates the credential vault.
Security Operations	Reviews privileged sessions and alerts.
Trust Center Coordinator	Keeps shared copies labeled as fictional.

The following RACI is illustrative.

Illustrative RACI for privileged access:

Activity	Privileged User	Privilege Approver	Vault Custodian	InfoSec Ops
Request elevation	R	A	I	I
Issue credentials	I	C	R	I
Perform elevated task	R	I	I	C
Review sessions	I	I	C	R
Review inventory	I	C	R	A

5. Policy Requirements and Controls

PTT-POL-005-C01. Maintain a privileged account inventory

Every elevated account is recorded with its owner and purpose, so the population of high-value accounts is known and bounded. An environment that cannot list its privileged accounts cannot protect them. The inventory is reconciled against actual accounts monthly.

PTT-POL-005-C02. Approve elevation separately

Granting or elevating privilege requires an approval independent of the requester, preventing a single person from self-authorizing. The approver is a different role from the user. Elevation requires a separate approval, so a routine session cannot silently gain privilege.

PTT-POL-005-C03. Use just-in-time access

Elevated rights are granted for a task and removed when the task ends, shrinking the window where privilege exists. Standing privilege is the exception, not the default. A report confirms privilege expired when the window closed.

PTT-POL-005-C04. Log privileged sessions

Commands and actions in privileged sessions are recorded so that misuse can be reviewed after the fact. The log is the deterrent and the audit trail. A sample of sessions is reviewed each month.

PTT-POL-005-C05. Use break-glass sparingly

Break-glass accounts are stored securely, used only in emergencies, and reviewed after each use, so the emergency path does not become a routine back door. Break-glass is the exception, not the routine, and every use is reviewed after the fact.

PTT-POL-005-C06. Review privileged access frequently

The inventory and its members are revalidated on a short cadence so stale privilege does not accumulate and former administrators do not retain rights. Privilege is re-confirmed more often than standard access, because it carries more risk.

PTT-POL-005-C07. Separate privileged and standard work

Daily work is performed in standard accounts, and elevated accounts are used only for elevated tasks, reducing the chance that routine activity carries unnecessary rights. A privileged task runs in a separate context, so routine browsing cannot be done with privilege.

PTT-POL-005-C08. Vault credentials

Privileged credentials are held in a controlled vault, not in shared documents or personal notes, so they cannot leak through casual channels. A check confirms no privileged credential sits outside the vault.

PTT-POL-005-C09. Rotate privileged credentials

Privileged passwords and tokens are rotated on a defined schedule and after any suspected compromise, limiting the value of a leaked credential. Rotation is verified by the vault's rotation log.

PTT-POL-005-C10. Alert on abnormal use

Unusual privileged activity, such as off-hours elevation, generates an alert for review so that anomalous behavior is caught quickly. Privileged activity outside the baseline raises an alert, so unusual use is caught.

PTT-POL-005-C11. Segregate privilege tiers

Privilege is divided into scoped and full tiers so that most administrators hold rights limited to one service rather than broad rights. Tiering shrinks the blast radius of any single compromised administrator. Tiers are separated so a compromise of one tier does not grant the tier above it.

PTT-POL-005-C12. Require justification at each elevation

Every elevation request carries a business justification, so privilege is granted for a reason rather than by habit. The justification is part of the approval record. Elevations without a recorded reason are counted and reviewed.

PTT-POL-005-C13. Monitor the vault

Access to the credential vault is itself logged and alerted on, so the store of keys is watched as closely as the keys themselves. Vault access is logged and reviewed, so the vault itself is not an unchecked path.

PTT-POL-005-C14. Bound the blast radius

Privilege is scoped so a compromised administrator can reach only the systems their role requires, limiting the damage of any single account. Privilege is scoped to the minimum surface, so a compromise reaches as little as possible.

PTT-POL-005-C15. Review privilege requests for necessity

Each elevation request is reviewed for whether the task actually needs the requested privilege, so privilege is not granted by habit. A request is checked for whether a lower-privilege option would suffice.

PTT-POL-005-C16. Report privileged access metrics

The standing-privilege count and just-in-time coverage are reported, so the program can see whether privilege is shrinking or growing. The metrics cover elevation count and review results, so the program's health is visible.

PTT-POL-005-C17. Minimize standing privilege

Elevated rights are granted for a bounded task and then removed, rather than left in place indefinitely, because standing privilege is the inventory an attacker mines. The default is no standing privilege, with temporary elevation requested per task. Standing privilege is measured and trending down.

PTT-POL-005-C18. Alert on privileged account creation

The creation or modification of a privileged account generates an immediate alert, so an attacker who manages to create their own back door announces the act instead of working silently. A new privileged account raises an alert, so creation is not silent.

PTT-POL-005-C19. Review privileged activity against baseline

Privileged actions are compared against a baseline of normal activity, and deviations are reviewed, because anomalous elevated behavior is the strongest single signal of a live compromise. Activity is compared to the baseline, and a deviation is investigated.

PTT-POL-005-C20. Record the elevation reason

Every privileged access elevation records the reason, so a later review sees why the access was granted, not just that it was. A monthly sample confirms the reason field is populated.

6. Operating Procedures

Request elevation.

The requester states the task, systems, and duration of the elevation, providing enough detail for an informed approval.

Obtain independent approval.

A privilege approver reviews and approves the request, and the decision is recorded.

Grant time-bound access.

Elevation is issued for the approved window only, with the expiry set at grant time.

Perform the task.

Actions stay within the approved scope and are logged throughout the session.

Revoke on completion.

Elevated rights are removed when the window closes, and the revocation is logged.

Review the inventory.

The Privileged Access Lead revalidates members and purposes on schedule and removes unneeded accounts.

Rotate credentials.

Privileged credentials are replaced on the scheduled interval or after a compromise.

Review sessions.

Security Operations reviews logged sessions for anomalies and follows up on anything unusual.

Issue a scoped credential.

The vault custodian issues a credential scoped to the single service the task requires, and the scope is recorded.

Rotate after break-glass.

Break-glass credentials are rotated immediately after use, and the rotation is logged.

Review a request for necessity.

The approver confirms the task needs the requested privilege before approving.

Report privilege metrics.

Standing-privilege and just-in-time coverage are reported on the cadence.

Check out a privileged credential.

The user requests access to a specific target, the request is tied to a task, the credential is released from the vault, and it is rotated on check-in.

Review a recorded session.

A reviewer replays or reads the session record against the stated justification and flags any action that exceeded the task scope.

Grant temporary elevation.

The requester cites the task, the elevation is granted with a time limit, and it expires automatically at the stated end.

Record a privilege elevation.

The approver records the reason, the scope, and the expiry, so a later review sees why the access was granted.

Review privileged entitlements.

The owner re-confirms each entitlement against current need and removes any that no longer apply.

Require a second approver for standing privilege.

A second reviewer signs off before any account keeps elevated rights beyond a single work session, so no single person can approve their own ongoing access. The approver records the business need and the intended review date.

Disable dormant accounts.

The access owner reviews accounts that have not authenticated with elevated rights for a defined period and disables or removes the privilege. The action is logged with the account name, the reason, and the reviewer.

Notify on credential compromise.

When a privileged credential is suspected or confirmed compromised, the owner disables it immediately, forces a reset, and records the affected systems for review.

7. Frequency and SLAs

Illustrative privileged-access cadence:

Activity	Frequency (illustrative)
Privileged access review	Monthly
Credential rotation	Every 90 days or on compromise
Session review	Sampled monthly
Inventory review	Monthly

8. Exceptions and Lifecycle

An exception permits standing elevated access for a narrowly defined fictional role, such as a monitoring service, when the Privileged Access Lead documents the necessity and adds compensating logging and review.

Standing exceptions are reviewed at least quarterly, and any standing privilege that is no longer necessary is revoked. Break-glass use is always reviewed after the fact, not treated as a routine exception.

Break-glass use is always reviewed after the fact and is never treated as a routine exception, because the emergency path is the one most likely to be abused precisely when oversight is weakest.

9. Records and Evidence

Record type	What it demonstrates (illustrative)
Privileged account inventory	The bounded list of elevated accounts.
Elevation requests	The task, systems, and duration requested.
Approval records	The independent approval decision.
Session logs	The recorded privileged activity.
Break-glass use records	Each emergency use and its review.
Rotation records	The scheduled credential replacements.
Scoped credential records	The issued credentials with their scope.
Vault access logs	The monitored access to the credential store.
Vault checkout log	The record of privileged credential use and rotation.
Session recordings	The captured privileged sessions.
Entitlement review records	The re-certification outcomes and revocations.
Elevation log	The recorded elevations with their reasons and expiries.
Vault access log	The recorded checkouts from the vault.
Administrator inventory	The maintained list of administrator accounts.
Elevation records	The recorded temporary grants.
Dormant account report	Shows each dormant privileged account, the last used date, and the action taken.
Recertification records	List each periodic re-approval of privileged access with the approver and date.
Compromise handling record	Documents the credential, the action taken, and the systems reviewed.

10. Oversight and Metrics

- Just-in-time coverage: the fraction of elevations that are time-bound rather than standing (illustrative).
- Standing privilege count: trending down.
- Session review completion: 100 percent of sampled sessions reviewed.
- Break-glass use: each use reviewed within the illustrative window.
- Scoped privilege coverage: the fraction of elevations scoped to one service rather than full.
- Privileged credential rotation: 100 percent rotated within the defined window.
- Session review coverage: the share of privileged sessions reviewed on schedule.
- Percentage of elevations with a recorded reason.

- Number of unnecessary entitlements removed per review.
- Sessions recorded versus total.
- Vault checkouts without a justification.
- Administrators reviewed on schedule.
- Elevations without a recorded reason.

11. Appendix

Illustrative privilege tiers:

Tier	Access (illustrative)
Standard	No elevated rights
Scoped admin	Elevated rights limited to one service
Full admin	Broad elevated rights, time-bound and logged
Break-glass	Emergency only, reviewed after use

12. Related Policy Dependencies

- Identity and Authentication Policy (governs the underlying accounts)
- Security Access Policy (defines customer-environment access)
- Logging and Monitoring Policy (captures privileged session events)
- Secure Configuration Policy (the settings privileged users may change)
- Encryption and Key Management Policy (governs the keys privileged users protect)

13. Review Cadence

The Privileged Access Lead reviews this policy at least annually, after a change to the illustrated privilege model, and after any significant simulated privileged misuse.

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-005
Document Owner	Privileged Access 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