

PAPER TIGER TECHNOLOGIES

Identity and Authentication Policy

1. Purpose

The purpose of this Identity and Authentication Policy is to define how identities are created, authenticated, reviewed, and removed in the PaperTiger demonstration. It sets the authentication requirements that make sure an account is used only by the person it belongs to.

Identity is the foundation of every access decision. If an account can be shared, guessed, or left active after departure, every downstream control that reasons about who did what becomes unreliable. This policy therefore governs the entire identity lifecycle, not just the login step.

This policy is fictional and illustrative. It describes no real identity, credential, or authentication system.

The policy treats authentication strength as proportional to risk: a standard account needs a password and a second factor, while a privileged or service account needs more. That scaling keeps the burden light where it can be and heavy where it must be.

Authentication is the front door, so the policy raises the bar on the factor itself, not just on the password, and keeps the door's opening and closing visible in logs.

The identity layer is only as strong as its weakest factor, so the policy pushes the environment toward phishing-resistant authentication and treats every sign-in anomaly as a signal worth chasing.

Authentication exists to confirm who is acting, and the policy makes identity a governed lifecycle rather than a pile of credentials.

2. Definitions

Term	Definition (illustrative)
Identity	The fictional record that ties an account to a single person or service.
Authentication	The process of proving an account is being used by its owner.
Multi-factor authentication	A second factor in addition to a password, such as an illustrative one-time code.
Least privilege	The practice of granting the minimum access needed for a task.
Provisioning	The creation and assignment of an account.

Offboarding	The removal of access when a person leaves or a service retires.
Service account	A machine identity used by an automated process rather than a person.
Access review	The periodic revalidation of whether an account still matches its role.
Break-glass account	An emergency account used only when normal access is unavailable.
Credential rotation	The scheduled replacement of a password or token.
Identity lifecycle	The stages from provisioning through offboarding.
Recovery path	The authenticated route to reset a lost credential.
Orphaned account	An account whose owner has left but which remains active.
Single sign-on (SSO)	The mechanism that lets a participant authenticate once and reach multiple illustrated systems without re-entering credentials.
Phishing-resistant factor	An authentication factor, such as a hardware key or platform passkey, that resists interception and impersonation attempts.
Session	The authenticated connection a participant holds after sign-in, which carries a defined idle and absolute lifetime.
Account takeover	The unauthorized use of a participant's account after their credentials have been obtained by another party.
Impossible travel	Authentication from two locations too far apart to be real.
Single sign-on	The use of one identity to reach many systems.
Federation	The trust between an identity provider and a service.
Session token	The credential that represents an authenticated session.

3. Scope and Boundaries

This policy applies to all fictional human and service identities that authenticate to the illustrated platform, tools, and supporting systems. It covers the full lifecycle from provisioning through offboarding.

It applies to workforce accounts, privileged accounts, and machine identities alike, with authentication strength scaled to the risk of the account rather than applied uniformly.

Out of scope are real identities, real credentials, and real authentication systems. This policy creates no real access and no real obligation.

Machine identities are in scope on equal footing with human ones, because a service account with broad rights is a higher-value target than a standard human account and is treated accordingly.

The escalation for authentication events follows a fixed chain: a detected anomaly goes first to the authentication administrator, then to the Information Security Lead if the anomaly is unresolved, and finally to the governance forum when a compromise is confirmed. Each step is logged so the handoff is visible.

Identity and authentication are fictional and illustrate the shape of real account governance.

4. Roles and Responsibilities

Role	Illustrative responsibility
Identity and Access Lead	Owns the policy and the identity lifecycle.
Access Administrator	Provisions, modifies, and revokes accounts per approved requests.
Account Owner	Uses credentials responsibly and reports suspected compromise.
Manager	Approves access requests and confirms role changes.
Security Operations	Investigates suspected account compromise.
Trust Center Coordinator	Maintains the fictional label on shared copies.

The following RACI is illustrative.

Illustrative RACI for the identity lifecycle:

Activity	Account Owner	Manager	Access Admin	InfoSec Lead
Request an account	R	A	I	I
Provision the account	I	I	R	C
Review access	C	R	C	A
Offboard	I	C	R	I
Rotate credentials	R	I	C	I

5. Policy Requirements and Controls

PTT-POL-004-C01. Use unique identities

Each account maps to one individual or one service, and shared human accounts are not used. Uniqueness is what makes an action attributable, and without it no log entry can be tied to a specific person. Each identity maps to one person, and shared accounts are prohibited.

PTT-POL-004-C02. Enforce multi-factor authentication

Human accounts require a second factor before first use of the platform, so a stolen password alone is not enough. The second factor is registered before the account is considered active. A report confirms no account is exempt without a documented exception.

PTT-POL-004-C03. Set password requirements

Passwords meet a defined minimum length and are not reused from other systems, reducing the chance that a breach elsewhere unlocks this environment through credential reuse. A composition check rejects a weak password at set time.

PTT-POL-004-C04. Provision by least privilege

Accounts start with the minimum role needed for the task, so a new account cannot immediately reach sensitive data and access grows only as the role requires. A new account starts with the minimum it needs and gains more only with a documented need.

PTT-POL-004-C05. Remove access on departure

Offboarding revokes access on the same business day in the demo, closing the window where a departed account remains usable. Revocation is triggered from the identity source. Departure revocations are reconciled against the HR list monthly.

PTT-POL-004-C06. Review accounts periodically

Access is revalidated against current role needs on a defined cadence so that accumulated, no-longer-needed access is removed rather than left in place. The review output is dated and a gap is remediated.

PTT-POL-004-C07. Protect service identities

Service accounts use scoped credentials and are inventoried and rotated on a schedule, because machine credentials are often the least watched and the most durable. Service credentials are confirmed in the secrets manager, not in code.

PTT-POL-004-C08. Handle break-glass carefully

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

PTT-POL-004-C09. Log authentication events

Successful and failed logins are logged so that anomalies such as repeated failures can be detected and investigated. The log captures success and failure alike, and a failure spike is flagged.

PTT-POL-004-C10. Suspend on compromise

A suspected compromised account is disabled immediately and reissued after verification, minimizing the time a compromised account remains usable. A compromised account is disabled immediately and re-authenticated before return.

PTT-POL-004-C11. Apply identity lifecycle governance

The full lifecycle from provisioning to offboarding is governed by this single policy so no stage is handled by a different, unstated rule. Consistency across the lifecycle prevents gaps at the seams between stages.

PTT-POL-004-C12. Protect recovery paths

Account recovery is itself authenticated, so the recovery path cannot be used to bypass the authentication it is meant to restore. Recovery is logged and reviewed. Recovery is gated to prevent an attacker from using the recovery path to take over an account.

PTT-POL-004-C13. Manage identity data minimally

Only the identity attributes needed for authentication and access are collected, so the identity store does not accumulate unnecessary personal data.

PTT-POL-004-C14. Govern federation

Federated authentication is configured to enforce the same multi-factor and session rules as direct login, so a federated path does not weaken the standard. Federated sign-in is limited to trusted identity providers, and the trust is reviewed.

PTT-POL-004-C15. Manage session controls

Session timeouts and re-authentication are enforced, so a forgotten session does not remain usable indefinitely. Sessions expire, and a long-idle session is closed rather than left open.

PTT-POL-004-C16. Protect against credential stuffing

Login monitoring and throttling limit automated attempts, so a list of leaked passwords cannot be tried at speed against the environment. A burst of failed logins triggers a lockout or a challenge, so a stuffing attack is slowed.

PTT-POL-004-C17. Require phishing-resistant authentication

Access to sensitive illustrated systems uses a phishing-resistant factor wherever available, because one-time codes and SMS can be intercepted. The factor choice is recorded so the authentication strength is visible. High-value access uses a factor that resists a phishing site, not just a password.

PTT-POL-004-C18. Bound session lifetimes

Sessions are limited by both an idle timeout and an absolute maximum, and they end on sign-out, because a session that stays open indefinitely turns a stolen device into a standing credential. A session has a maximum lifetime, and re-authentication is required beyond it.

PTT-POL-004-C19. Lock accounts after repeated failure

Repeated failed sign-in attempts trigger a temporary lock or escalating challenge, so automated guessing is slowed before it succeeds. The lock threshold is set low enough to stop guessing without creating an easy denial-of-service path. The lockout threshold and duration are documented and tested.

PTT-POL-004-C20. Require re-authentication for sensitive actions

A participant must re-authenticate before performing an action that changes credentials, grants access, or moves data, so a hijacked session cannot silently escalate. The re-prompt breaks the reuse of a stolen session token. A sensitive action prompts a fresh factor check, so a hijacked session cannot act freely.

PTT-POL-004-C21. Detect and flag impossible travel

Sign-in attempts that cannot be explained by physical travel are flagged for review, because a credential appearing in two distant places within minutes is a reliable sign of compromise. The flag triggers a challenge or a temporary lock rather than silent admission. A flagged event is reviewed by a human before it is dismissed.

PTT-POL-004-C22. Bind authentication to enrolled devices

Sensitive access is tied to devices that have been enrolled and verified, so a stolen password alone is not enough to reach the environment from an unknown endpoint. A new device must be enrolled before it can authenticate, so an unknown device is refused.

6. Operating Procedures

Request an account.

The requester names the role, business need, and approving manager. The request is retained as the record of why access was granted.

Verify and provision.

The Access Administrator confirms approval and creates the account with least privilege, applying the role rather than a broad default.

Enroll a second factor.

The account owner registers a second factor before first login, and the enrollment is recorded.

Review access.

Managers confirm each account still matches the current role on the review cadence, and mismatches are corrected.

Revoke on departure.

Offboarding triggers revocation and a record of the removal, with the same-business-day target applied.

Rotate service credentials.

Machine credentials are replaced on their scheduled interval and the rotation is logged.

Respond to compromise.

A suspected compromise triggers immediate suspension and a reissue after verification.

Record the lifecycle.

Each lifecycle event is logged for audit and review so the identity's history is reconstructable.

Handle a recovery request.

A recovery request is verified through a pre-registered factor before any credential is reset, and the recovery is logged.

Reconcile the identity store.

The identity store is compared against the active workforce on a cadence, and orphaned accounts are removed.

Configure federation.

Federated authentication is configured to inherit the multi-factor and session rules.

Review login anomalies.

Repeated failures and unusual patterns are reviewed and investigated.

Enroll a phishing-resistant factor.

The participant registers a hardware key or passkey, the factor is bound to their account, and a fallback path is recorded for the case where the factor is lost.

Reset a forgotten credential.

The participant proves their identity through a secondary verified channel, the credential is reset, and prior sessions are invalidated to cut off any lingering access.

Handle an impossible-travel flag.

The sign-in is challenged or paused, the account owner is notified, and the event is reviewed to confirm whether the activity was legitimate.

Review account ownership.

The owner re-confirms every account to a current person and disables any orphan.

Suspend a compromised account.

The administrator disables the account, forces a re-authentication, and logs the event.

7. Frequency and SLAs

Illustrative identity cadence:

Activity	Frequency (illustrative)
Access review	Quarterly
Service credential rotation	Every 90 days
Password change	On compromise or policy trigger
Offboarding revocation	Same business day

8. Exceptions and Lifecycle

An exception permits a temporary delay, such as a short extension of a departing contractor's access for handoff, when the Identity and Access Lead documents the reason, the duration, and the monitoring applied.

Exceptions expire automatically and are reviewed quarterly. An exception that extends access beyond a departure is the highest-scrutiny case and requires an additional compensating control such as session monitoring.

An exception that extends access beyond a departure is the highest-scrutiny case and requires session monitoring, because it is the exact scenario the offboarding control exists to prevent.

9. Records and Evidence

Record type	What it demonstrates (illustrative)
Account request records	The role, need, and approver for each account.
Provisioning logs	The created and assigned accounts.
MFA enrollment records	Confirmation of second-factor registration.
Access review output	The revalidation of account-to-role fit.
Offboarding records	Revocation and removal evidence.
Authentication logs	Successful and failed login events.
Recovery records	The verified and logged recovery events.
Identity store reconciliation	The comparison of accounts to active workforce.
Factor enrollment records	The phishing-resistant factors bound to each account.
Authentication event logs	Sign-in and failure records.
Account lock records	The lockout events and their resolutions.
Account review results	The dated re-confirmations of ownership.
Suspension records	The dated account suspensions and reasons.
Federation trust records	The documented identity-provider trusts.
Session policy	The configured session lifetime and idle rules.

10. Oversight and Metrics

- MFA coverage: 100 percent of human accounts enrolled (illustrative).
- Offboarding timeliness: revocation within one business day in the demo.
- Access review completion: 100 percent of due reviews completed.
- Shared account count: zero shared human accounts.
- Orphaned accounts: zero active accounts without a current owner.
- Authentication failure rate: failed sign-ins against total trending flat with no unexplained spikes.
- Phishing-resistant coverage: the share of sensitive accounts enrolled trending upward.
- Orphaned accounts at each review.
- Time from compromise report to suspension.
- Federation trusts reviewed on schedule.
- Session lifetime violations.

11. Appendix

Illustrative authentication tiers:

Tier	Requirement (illustrative)
Standard workforce	Password plus a second factor
Privileged	Password, second factor, and separate approval

Service account	Scoped machine credential with automated rotation
-----------------	---

12. Related Policy Dependencies

- Privileged Access Policy (governs the elevated subset of identities)
- Security Access Policy (defines customer-environment access)
- Asset Management Policy (inventories the devices identities authenticate from)
- Logging and Monitoring Policy (captures authentication events)
- Acceptable Use Policy (governs how accounts are used)

13. Review Cadence

The Identity and Access Lead reviews this policy at least annually, after a change to the illustrated authentication stack, and after a significant simulated account compromise.

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-004
Document Owner	Identity and 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