APONO

Checklist

Zero Standing Privileges Checklist

This checklist helps you quickly evaluate the strength of your identity and access security program and uncover where standing privileges, weak controls, or governance gaps may still exist. Use it to identify priorities and chart a clear path toward Zero Standing Privileges.

Category	Checklist Item	Status	Notes
Identity Foundations	All users authenticate through centralized SSO/IdP	☐	
	MFA required for all user accounts including admins	☐	
	All service accounts and API keys have clear owners	☐	
	Only individual identities allowed and not shared accounts	☐	
	Non-human identities are inventoried and documented	☐	
	Every identity has a defined purpose and justification	☐	
	Default permissions for new identities are restrictive	☐	
	No orphaned or unassigned accounts exist	☐	
Least Privilege Access	No one retains admin access for day-to-day tasks	☐	
	Privileged roles are tightly scoped and not catch-all roles	☐	
	Production access is limited to defined personas and restricted with JIT access	☐	
	Granular access to storage (S3/GCS/Blob) is restricted to buckets/folders level	☐	
	Database access is scoped to schema/table/role level	☐	
	Environment separation enforced between dev/stage/prod	☐	
	Infrastructure access follows least privilege	☐	
ZSP Controls	High-risk permissions are not standing privileges	☐	
	Privileged access granted Just-in-Time when needed	☐	
	All JIT sessions are auto-expiring and time-limited	☐	
	Elevated access requires justification or ticket link	☐	
	Elevations follow approval workflows	☐	
	Temporary roles created on-demand then removed	☐	
	Break-glass access tightly controlled and logged	☐	
	Standing admin accounts replaced with JIT elevation	☐	
Fine-Grained Access	Access can be restricted to specific cloud resources	☐	
	Sensitive configuration changes require explicit elevation	☐	
	Read/write/modify/delete rights separated clearly	☐	
	NHI access scoped to specific services/functions	☐	
	Pipelines/automation do not have full environment access	☐	
	K8s access scoped by namespace/cluster/workload	☐	
	DB permissions reflect specific operations not blanket admin access	☐	
NHI Governance	Service accounts use short-lived or rotating credentials	☐	
	No broad service accounts	☐	
	No long-lived root keys	☐	
	NHI credentials have expiration when possible	☐	
	NHIs included in access review cycles	☐	
	CI/CD agents and data pipelines use least privilege roles	☐	
	NHIs tagged by owner and environment	☐	
	Dormant or unused NHIs automatically flagged	☐	
Access Lifecycle	Joiner/mover/leaver workflows update access automatically	☐	
	Role changes trigger privilege reevaluation	☐	
	Terminated users lose all access immediately	☐	
	Privilege reviews scheduled quarterly or more	☐	
	Reviews include humans and NHIs	☐	
	Privilege roles reviewed with evidence	☐	
	Privilege usage data included in reviews	☐	
	Review outcomes documented and audit-ready	☐	
Monitoring & Logging	All privileged actions logged centrally	☐	
	All JIT requests and approvals logged with context	☐	
	Logs link user identity resource and action	☐	
	Alerts exist for unusual privilege events	☐	
	SIEM receives identity and privilege events	☐	
	Privileged activity dashboards available	☐	
	Logs are immutable and long-term retained	☐	
	Logs correlated with access logs	☐	
Cloud & Infra Coverage	ZSP applied across AWS GCP Azure K8s D8s	☐	
	Least privilege applied across SaaS as well	☐	
	Multi-cloud access model is consistent	☐	
	Access policies managed via IaC, API or code	☐	
	Cloud roles auto-rightsized based on actual use	☐	
	Critical cloud operations require elevation	☐	
	Privileged cloud access is time-bounc and logged	☐	
	Privileged governance extends to on-prem/hybrid	☐	

About Apono

Founded in 2022 by Rom Carmel and Ofir Stein, Apono delivers a Cloud Privileged Access Platform purpose-built for modern, fast-moving environments. With support for both human and non-human identities, Apono helps security and DevOps teams enforce least privilege at scale without slowing down delivery.

Trusted by Fortune 500 enterprise and recognized in Gartner's Magic Quadrant for Privileged Access Management two years running, Apono is shaping the future of secure cloud access.

APONO

www.apono.io

@Apono_official

@Apono