

DSi Aeris AI Standards Policy

This document outlines the standard naming and governance framework for all Azure subscriptions and resources used in the Aeris AI Platform managed by DSi Professionals.

1. Naming Format Overview

All Azure resources follow a structured and consistent naming model:

<Proj>-<Env>-<Svc>-<Type>-<Seq>

Example: AER-PD-AI-STG01

| Segment | Description | Example |
|---------|---|--------------|
| Proj | Top-level project or platform code | AER |
| Env | Environment (Development, Test, Production) | DV / TS / PD |
| Svc | Primary service area (AI, DATA, SEC, OPS) | AI |
| Type | Resource type (VM, KV, STG, DB, RG, etc.) | STG |
| Seq | Sequence number (for duplicates) | 01 |

2. Azure Subscription Naming

| Purpose | Format | Example | Description |
|-------------------------|----------------|----------------|--|
| Core AI Platform | AER-AI-SUB-PD | AER-AI-SUB-PD | Primary production subscription for Aeris AI resources |
| Development | AER-AI-SUB-DV | AER-AI-SUB-DV | Development and testing environments |
| Sandbox / Lab | AER-AI-SUB-SB | AER-AI-SUB-SB | R&D and prototype experimentation |
| Operations & Monitoring | AER-OPS-SUB-PD | AER-OPS-SUB-PD | Dedicated subscription for operational tooling, logs, and SOC monitoring |

3. Environment Codes

| Environment | Code | Description |
|-------------|------|---|
| Development | DV | Used for internal development and test builds |
| Test | TS | Quality assurance and integration validation |
| Production | PD | Live operational Aeris AI systems |
| Sandbox | SB | Temporary or experimental builds |

4. AI and Data Resource Type Codes

| Code | Resource |
|------|---|
| AI | Azure AI Service (OpenAI, Cognitive, Custom Vision, etc.) |
| DB | Azure SQL / Cosmos / PostgreSQL Database |
| STG | Azure Storage Account (data, vector store, logs) |
| KV | Azure Key Vault (API keys, credentials, secrets) |
| APP | Web App, Container App, or Function |
| VM | Virtual Machine for compute or model hosting |
| NET | VNet or Subnet for AI components |
| RG | Resource Group |
| MON | Application Insights / Monitoring |
| ACR | Azure Container Registry |
| MLW | Machine Learning Workspace |
| AGW | Application Gateway |
| FW | Firewall |

5. Azure Hierarchy & Component Diagram Example



6. Tagging Standard

| Tag | Example | Description |
|-------------|-------------------|--|
| Project | Aeris AI | Identifies the overarching project |
| Environment | Production | Operational stage |
| Owner | DSi Professionals | Responsible organisation |
| Service | AI Platform | Functional service grouping |
| CostCentre | AI-001 | Optional internal tracking code |
| DataClass | Confidential | Data classification tag for compliance |

7. Governance Rules

The following governance standards apply to all Aeris AI Azure environments managed by DSi Professionals. These ensure consistency, operational security, and cost-effective management across all tenants and environments.

7.1 General Naming and Structure

1. All resource names must comply with the defined DSi naming standard (<Proj>-<Env>-<Svc>-<Type>-<Seq>).
2. Uppercase naming conventions are to be used across all Azure services and artefacts.
3. No spaces, special characters, or underscores are permitted.
4. Each environment (Development, Test, Production) must exist within its own Azure Subscription and Resource Group.
5. Shared services (e.g., monitoring, logging, networking) should be isolated under dedicated operational resource groups.

7.2 Security and Identity Management

1. All access to Azure resources must be managed through Microsoft Entra ID using role-based access control (RBAC).
2. Privileged accounts must require multi-factor authentication (MFA) and, where possible, conditional access policies.
3. Administrative actions should be logged centrally in Azure Monitor or Sentinel for audit tracking.
4. Service principals must use managed identities instead of static credentials or keys.
5. Key Vault resources (e.g., AER-TS-AI-KV01) must store all API tokens, keys, and certificates with proper rotation policies.
6. Network Security Groups (NSGs) and Azure Firewall policies must restrict access to approved IP ranges or virtual networks only.
7. All AI service endpoints (OpenAI, Cognitive, ML Workspaces) must be deployed using private endpoints and secured through Private Link.
8. Diagnostic logs and audit data must be retained for a minimum of 90 days, with automated transfer to long-term storage for compliance.

7.3 Cost and Resource Optimisation

1. All Development (DV) and Testing (TS) resources must implement auto-shutdown schedules during non-business hours (e.g., 7pm–7am local time).
2. Use Azure Automation Runbooks or Logic Apps to automatically deallocate unused VMs and AI compute resources.
3. Apply Azure Budgets and Cost Alerts at the subscription level to notify administrators of cost threshold breaches.
4. Enable Azure Advisor recommendations and review monthly for potential cost-saving actions.

5. All GPU-based AI workloads (training or inference) should use spot VMs for non-critical operations to reduce compute expenses.
6. Storage lifecycle management must automatically archive or delete aged logs and datasets beyond business retention requirements.

7.4 Operational Management and Automation

1. Implement Azure Policy definitions to enforce tagging, region restrictions, and security baselines.
2. Use Azure Blueprints for consistent deployment of governance artefacts across all environments.
3. Continuous compliance scans should be automated using Defender for Cloud and Azure Security Benchmark policies.
4. All deployments must be performed through approved CI/CD pipelines (e.g., GitHub Actions or Azure DevOps) with change tracking enabled.
5. Auto-scaling policies should be configured for all AI and web app resources to optimise availability and cost.
6. Schedule weekly automated patching for all managed VMs and container hosts using Azure Update Manager.
7. Enable resource locks on critical production resources (AI models, Key Vaults, storage) to prevent accidental deletion or modification.

7.5 Backup, Monitoring and Incident Response

1. All production storage and databases must have daily backups with geo-redundant recovery (GRS) enabled.
2. Configure Azure Monitor and Log Analytics Workspaces for centralised visibility across all Aeris AI subscriptions.
3. Alerts should integrate with DSi's SOC workflows for proactive issue escalation.
4. All incident logs must be retained for a minimum of 12 months for post-incident analysis.
5. Critical services must include a disaster recovery plan documented in the Aeris AI Configuration Register.