Rentola Azure Data Management Baseline Governance (handbook Section)

**Rentola — Azure Cloud Data Management Baseline Governance**

Version: 1.0  
Owner: Chief Information Security Officer (CISO) and Head of Data  
Review Cycle: Quarterly (Jan/Apr/Jul/Oct)  
Applies to: All Rentola employees, contractors, and vendors handling data in Azure and connected platforms

**1. Purpose, Scope, and Outcomes**

**Purpose.** Establish a clear, enforceable baseline for how Rentola discovers, classifies, protects, processes, shares, and retires data in Microsoft Azure.

**Scope.** All data created, collected, processed, or stored in Rentola-managed Azure tenants and subscriptions, including Azure Storage (Blob/Files), Azure Databases (SQL, PostgreSQL, Cosmos DB, MySQL), Synapse, Fabric, Data Explorer (ADX), Event Hubs, Stream Analytics, Databricks (if used), and connected SaaS (e.g., M365, Dynamics) when integrated with Azure.

**Outcomes.**

* Regulatory compliance (GDPR/DSG, ePrivacy, PCI-DSS if applicable) and contractual obligations.
* Reduced breach/exfiltration risk; improved resilience and recoverability.
* Traceable data lineage and accountable ownership.
* Consistent lifecycle management and cost-optimized storage.

**Non-goals.** This baseline does not replace product-specific standards (e.g., PCI, medical), which may impose stricter controls.

**2. Roles & Responsibilities (RACI)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Role** | **Responsibility** | **R** | **A** | **C** | **I** |
| **Data Owner** (business) | Defines purpose, classification, retention; approves access | R | A | CISO, DPO, Data Steward | Security, Engineering |
| **Data Steward** (operational) | Catalogs metadata, quality rules, lineage in Purview | R |  | Data Owner | Engineering |
| **CISO** | Security policy, risk acceptance, incident response oversight |  | A | Data Owner, DPO | All |
| **DPO/Privacy** | DPIA, lawful basis, data subject rights |  | A | Data Owner | All |
| **Platform Engineering** | Azure landing zone, policy-as-code, monitoring | R |  | CISO | All |
| **Security Operations (SecOps)** | Detection, response, forensics | R |  | CISO | All |
| **Developers/Data Engineers** | Implement controls in code/pipelines | R |  | Platform | Data Owner |
| **Third Parties** | Contractual adherence, technical integration | R |  | Data Owner, CISO | Legal |

**Key principles.** Single data owner per dataset; no orphaned data; least privilege; Zero Trust; everything codified.

**3. Data Classification & Handling Rules**

Rentola data must be labeled and handled according to sensitivity, impact, and regulatory constraints.

**3.1 Classification Levels**

1. **Public** — Approved for public dissemination.
2. **Internal** — Business-as-usual internal use; no public disclosure.
3. **Confidential** — Business-critical, commercially sensitive, or personal data (non-special-category).
4. **Restricted** — Special-category personal data, secrets (keys, tokens), financial reporting, legal hold, or data subject to heightened regulation (e.g., payment data).

**3.2 Labeling & Tagging**

* **Purview Sensitivity Labels**: Public, Internal, Confidential, Restricted (+ optional regional qualifiers, e.g., EU-Only).
* **Azure Resource Tags** *(mandatory on all data-bearing resources)*:
  + DataClassification={Public|Internal|Confidential|Restricted}
  + DataOwner=<email>
  + RetentionPolicy=<name>
  + BusinessUnit=<name>
  + PII={Yes|No}
  + RegionScope={EU-Only|Global}
  + CostCenter=<code>

**Enforcement:** Azure Policy to **deny** creation of storage/db resources without tags; Audit-if-not-exists for legacy.

**3.3 Handling Matrix (excerpt)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Classification | Allowed Locations | Encryption | Access | Sharing | Retention |
| Public | Any approved region | SSE (platform) | AuthN required for writes | Public read only via fronted services/CDN with WAF | As defined |
| Internal | Primary region(s) | SSE + TLS1.2+ | RBAC via Entra ID | Internal tenants only; no public endpoints | As defined |
| Confidential | EU regions only unless approved | CMK (Key Vault/HSM) + TLS1.2+ | PIM + CA + device compliance | Private Endpoints; egress via approved brokers | Min. 2–7 yrs per domain |
| Restricted | EU regions; specific landing zones | CMK with HSM; Double encryption where feasible | Break-glass only; JIT; step-up MFA | No external unless DPA/SCC; private link | Legal hold + domain policy |

**4. Data Architecture & Storage Patterns**

**Approved services**

* **Object/Files**: Azure Blob (Hot/Cool/Archive), Azure Files with Private Endpoints
* **Relational**: Azure SQL Managed Instance/DB; Azure Database for PostgreSQL/MySQL (Flexible Server)
* **NoSQL**: Cosmos DB (Core/Gremlin/Cassandra) with private link and RBAC
* **Analytics**: Azure Synapse/Fabric Lakehouse, ADLS Gen2, Data Explorer (ADX)
* **Secrets**: Azure Key Vault (Premium/HSM where needed)

**Mandatory controls**

* Disable **public network access** for data services; use **Private Endpoints** and **service endpoints** where applicable.
* **Firewall rules** default deny; allow only trusted subnets via Azure Firewall and NSGs.
* **Cross-tenant** data movement requires CISO/DPO review and data-sharing agreement.
* **Geo-Redundancy**: Select LRS/ZRS/GRS/RA-GRS based on Criticality Tier (see 7.4).

**Naming convention (examples)**

* Storage account: st<env><region><app><purpose> e.g., st-prd-weu-rntl-orders
* Key Vault: kv-<env>-<region>-<domain> e.g., kv-prd-weu-identity
* ADLS container: <domain>-<zone> e.g., orders-raw, orders-curated

**5. Identity, Access, and Key Management**

**Identity & Access**

* Entra ID as single IAM plane; disable local DB users where possible; prefer **Managed Identities**.
* **RBAC** over data-plane roles: Reader, Data Reader/Contributor, Storage Blob Data roles; **no Owner at subscription** except break-glass.
* **Privileged Identity Management (PIM)** for elevation; **JIT** approval with ticket reference.
* **Conditional Access**: MFA required; device compliance for Restricted/Confidential; location-based policies for admin roles.
* **Access Reviews**: Quarterly for Confidential; monthly for Restricted datasets.

**Key Management**

* **CMK** stored in **Key Vault Premium** (HSM-backed) for Confidential/Restricted; rotate every 180 days minimum.
* Enable **Key Vault firewall** + Private Endpoints; disallow public network.
* Use **soft delete** and **purge protection** on Key Vaults.
* Separation of duties: Key admins ≠ data admins.

**6. Data Lifecycle & Retention**

**Lifecycle states**: *Ingest → Process → Store → Use/Share → Archive → Dispose*.

**Retention policy examples (baseline)**

* Finance transactions: **7 years** (statutory)
* Customer support tickets (PII): **3 years** after last interaction
* Access logs/audit: **1 year** online + **6 years** cold archive
* Secrets/keys: Rotate as per 5; retain logs **forever** under legal hold if incident

**Automation**

* **ADLS/Blob lifecycle rules** to tier blobs (Hot→Cool→Archive) and auto-delete per container label.
* **SQL**: Use long-term retention (LTR) backups per tier (e.g., weekly full 12 weeks, monthly full 7 years for Finance).
* **Purview**: Use classifications to drive retention in Microsoft 365 and downstream systems.

**Disposal**

* Irreversible deletion using secure wipe API; generate **Disposition Certificate** approved by Data Owner.

**7. Backup, Recovery, and Resilience**

**Backup**

* Azure Backup for VMs/Files/SQL; application-consistent snapshots; encrypted backups with CMK.
* **Immutable Backups** (Blob immutability policy / MARS vault with immutability) for Restricted datasets.

**Recovery**

* RPO/RTO tiers:
  + Tier 0 (Restricted): RPO ≤ 15 min, RTO ≤ 1 hr
  + Tier 1 (Confidential): RPO ≤ 1 hr, RTO ≤ 4 hrs
  + Tier 2 (Internal/Public): RPO ≤ 24 hrs, RTO ≤ 24 hrs

**DR Strategy**

* Primary in **West Europe (WEU)**; secondary in **North Europe (NEU)** unless data residency constraints.
* Failover tested **semi-annually**; document runbooks.

**Platform Resilience**

* Zonal services preferred; use ZRS for storage where available; health probes and autoscaling on data gateways.

**8. Data Movement, Sharing, and Egress Control**

**Approved movement**

* **Private**: ADF/Synapse Pipelines via Private Endpoints, Event Hubs, Service Bus, ExpressRoute.
* **Streaming**: Event Hubs/ADX with network isolation.
* **Integration**: Azure API Management (internal), B2B via Entra External Identities.

**Prohibited patterns**

* Public SAS tokens without expiration; anonymous access to containers.
* Ad-hoc exports to personal storage or unsanctioned SaaS.

**Egress control**

* Azure Firewall with FQDN tags; allow-list only; DNS proxy + Private DNS zones.
* DLP via Defender for Cloud Apps for SaaS egress; Purview DLP for M365.

**Data Sharing Agreements**

* Mandatory for third parties: purpose limitation, retention, deletion, breach notice ≤72h, SCCs where required.

**9. Monitoring, Logging, and Analytics**

**Diagnostics (mandatory categories)**

* **Storage**: Read/Write/Delete, BlobCreated, BlobDeleted, ListBlobs, SetBlobTier, PutBlob.
* **Databases**: Query Store, Connection audit, Failed/Succeeded logins, Threat detection.
* **Key Vault**: Secret/Get, Secret/Set, Key/Wrap/Unwrap, Access policy changes.

**Centralization**

* Send all diagnostics to **Log Analytics**; stream to **Microsoft Sentinel** for detection.

**High-value detections**

* Unusual download velocity; mass tier changes (Hot→Archive); public network re-enablement; key vault purge attempt; SAS tokens with excessively long TTLs; cross-tenant sharing spikes.

**Dashboards & KPIs**

* % resources with mandatory tags (target ≥ 98%)
* % services with public access disabled (target 100%)
* Key rotation age ≤ 180 days (target 100%)
* Access review completion within SLA (target 100%)

**10. Privacy, DPIA, and Data Subject Rights (DSR)**

**Lawful basis & DPIA**

* Every Confidential/Restricted dataset must document lawful basis and, if high risk, a **Data Protection Impact Assessment (DPIA)**.

**Data Subject Rights**

* Provide export/delete within statutory timelines; Purview catalog IDs used to locate datasets; use Fabric/Synapse/ADF scripted jobs for subject data discovery across zones.

**Minimization & Pseudonymization**

* Default to column-level encryption/tokenization for PII; differential privacy techniques in analytics where feasible.

**11. Policy-as-Code (Azure Policy) — Baseline Set**

**ALZ Policy Set** (assign at management group mg-rentola-landingzones):

1. **Deny public network access** for Storage, SQL, Cosmos DB.
2. **Require Private Endpoint** for data services in Prod.
3. **Enforce HTTPS** and TLS ≥ 1.2 for storage and web endpoints.
4. **Require CMK** for Storage Accounts labeled Confidential/Restricted.
5. **Require resource tags** (DataClassification, DataOwner, PII).
6. **Audit diagnostic settings** to Log Analytics.
7. **Deny creation** of storage accounts without allowSharedKeyAccess=false.

**Sample Policy – Deny Public Blob Access**

{

"properties": {

"displayName": "Deny public blob access",

"policyType": "Custom",

"mode": "All",

"parameters": {},

"policyRule": {

"if": {

"allOf": [

{"field": "type", "equals": "Microsoft.Storage/storageAccounts"},

{"field": "Microsoft.Storage/storageAccounts/allowBlobPublicAccess", "equals": true}

]

},

"then": {"effect": "deny"}

}

}

}

**Sample Policy – Require Tags**

{

"properties": {

"displayName": "Require data tags",

"policyType": "Custom",

"mode": "Indexed",

"parameters": {},

"policyRule": {

"if": {"field": "type", "in": [

"Microsoft.Storage/storageAccounts",

"Microsoft.Sql/servers",

"Microsoft.DocumentDB/databaseAccounts"

]},

"then": {"effect": "deny", "details": {

"type": "Microsoft.Resources/tags",

"existenceCondition": {

"allOf": [

{"field": "tags['DataClassification']", "exists": "true"},

{"field": "tags['DataOwner']", "exists": "true"},

{"field": "tags['PII']", "exists": "true"}

]

}

}}

}

}

}

**Storage Lifecycle Rule (example)**

{

"rules": [

{

"enabled": true,

"name": "tier-and-expire",

"type": "Lifecycle",

"definition": {

"filters": {"blobTypes": ["blockBlob"], "prefixMatch": ["orders-raw/"]},

"actions": {

"baseBlob": {

"tierToCool": {"daysAfterModificationGreaterThan": 30},

"tierToArchive": {"daysAfterModificationGreaterThan": 90},

"delete": {"daysAfterModificationGreaterThan": 1095}

}

}

}

}

]

}

**12. Operational Processes & Runbooks**

**12.1 Dataset Onboarding**

1. Submit intake form (purpose, lawful basis, owner, classification, region).
2. Create IaC module (Bicep/Terraform) using approved blueprints.
3. Assign Azure Policy and diagnostic settings.
4. Register in Purview (schema, glossary, lineage) and assign steward.
5. Enable backups, lifecycle rules, and key management.

**12.2 Access Provisioning**

* Request via ITSM; include dataset ID and role; PIM approval; time-bound; logged.

**12.3 Break-glass Access**

* Two named accounts kept in sealed vault; tested monthly; alert on use; post-incident review required.

**12.4 Data Sharing with Third Parties**

* DPA & DSA signed; security questionnaire; connectivity via private link; time-limited SAS (with IP and expiry ≤ 24h) if unavoidable.

**12.5 Decommissioning**

* Freeze writes; export required records; verify legal holds; secure wipe; update Purview; issue Disposition Certificate.

**13. Detection & Incident Response (Data Breach)**

**Triggers**: anomalous egress, unauthorized key operations, policy violations, mass permission grants.

**Playbook (condensed)**

1. **Detect & Triage**: Sentinel alerts; classify severity; open incident ticket.
2. **Contain**: Revoke SAS; disable public access; rotate keys/secrets; isolate subnets.
3. **Eradicate**: Patch misconfig, re-assign policy, fix IaC.
4. **Recover**: Restore from immutable backups; validate integrity.
5. **Notify**: DPO initiates regulatory and customer notices (≤72h if required).
6. **Lessons Learned**: PIR within 5 business days; update controls.

**Forensics**: Preserve Log Analytics workspace; export to secure storage; maintain chain of custody.

**14. Compliance Mapping (excerpt)**

* **GDPR/DSG**: Lawfulness (Art.6), DPIA (Art.35), DSR (Art.12–23), Security (Art.32), Breach (Art.33/34).
* **PCI-DSS** (if applicable): Network segmentation, key management, logging, vulnerability management for cardholder data environments.
* **ISO/IEC 27001**: A.5–A.8 (policies, roles, assets), A.9 (access), A.10 (crypto), A.12 (ops), A.14 (system acquisition), A.18 (compliance).

**15. Metrics, Audits, and Continuous Improvement**

**Key Metrics** (reported monthly):

* Policy compliance rate per control family.
* % datasets with assigned owner & steward.
* Mean time to remediate (MTR) policy drift.
* % datasets with complete lineage in Purview.

**Audit Cadence**

* Technical control review (monthly), Access reviews (quarterly), DR test (semi-annual), DPIA review (annual or upon change).

**Control Exceptions**

* Documented via risk register with expiry; CISO approval; compensating controls mandatory.

**Roadmap**

* Q1: Expand Purview auto-classification and lineage coverage ≥ 90% datasets.
* Q2: Confidential Compute pilots (SEV-SNP/TDX) for Sensitive analytics.
* Q3: Attribute-based access control (ABAC) via Purview/labels + Entra entitlement mgmt.
* Q4: Data Clean Room for privacy-preserving data collaboration.

**16. Appendices**

**A. Dataset Intake Template**

* Dataset name, purpose, owner, steward, legal basis, PII type, region, classification, retention, consumers, interfaces, IaC module ID.

**B. DSR Runbook (Summary)**

1. Verify identity of requester.
2. Locate datasets via Purview; run subject-data discovery scripts.
3. Export or erase per policy; record evidence; inform requester.

**C. Example Terraform/Bicep Snippets** *(abbreviated)*

resource "azurerm\_storage\_account" "this" {

name = "st-prd-weu-rntl-orders"

resource\_group\_name = azurerm\_resource\_group.rg.name

location = azurerm\_resource\_group.rg.location

account\_tier = "Premium"

account\_replication\_type = "ZRS"

allow\_blob\_public\_access = false

min\_tls\_version = "TLS1\_2"

shared\_access\_key\_enabled = false

tags = {

DataClassification = "Confidential"

DataOwner = "data.owner@rentola.com"

PII = "Yes"

}

}

resource st 'Microsoft.Storage/storageAccounts@2023-01-01' = {

name: 'st-prd-weu-rntl-orders'

location: resourceGroup().location

sku: { name: 'Standard\_ZRS' }

kind: 'StorageV2'

properties: {

minimumTlsVersion: 'TLS1\_2'

allowBlobPublicAccess: false

supportsHttpsTrafficOnly: true

networkAcls: {

defaultAction: 'Deny'

bypass: 'AzureServices'

virtualNetworkRules: [

{ id: subnetResourceId('vnet-core','subnet-data') }

]

}

}

tags: {

DataClassification: 'Confidential'

DataOwner: 'data.owner@rentola.com'

PII: 'Yes'

}

}

**D. Glossary**

* **CMK**: Customer-Managed Key.
* **PIM/JIT**: Privileged Identity Management / Just-In-Time access.
* **Purview**: Microsoft data governance and catalog service.
* **Private Endpoint**: Private IP mapped to PaaS service.
* **DPIA**: Data Protection Impact Assessment.

**Approval**  
CISO: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_  
Head of Data: \_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_