**Operational Runbook**

Data flow: Name (reduce line font size if required to avoid line break)

Updated: Month, Year

|  |  |  |
| --- | --- | --- |
| ***Essentials*** | |  |
| Release | | Number (Major.Minor) |
| Released | | DD.MM.YYYY |
| Data catalog updated | | DD.MM.YYYY |
| Developer(s) | | Shortname(s) |
| DevOps team | | Team name |
| **Source data** | Content | Brief description |
| location | Cloud/On-premises |
| type | Brief description |
| Technical contact person(s) | Shortname(s) |
| Subject matter expert(s) | Shortname(s) |
| **Data transfer** | type | Full/Delta |
| frequency | Weekly/Daily/Hourly/(higher frequency) |
| orchestration | System component type |
| Destination | OMNIA component type(s) |
| Criticality | High/Medium/Low |
| Security classification | Open/Internal/Restricted/Confidential |
| Gateway | System component name |

Contents

[1 Introduction 3](#_Toc5088407)

[1.1 Purpose 3](#_Toc5088408)

[1.2 Scope 3](#_Toc5088409)

[1.3 Authoring rules 3](#_Toc5088410)

[1.4 Legal 3](#_Toc5088411)

[2 Architecture 4](#_Toc5088412)

[2.1 Architecture overview 4](#_Toc5088413)

[2.2 Hardware 4](#_Toc5088414)

[2.3 Software 4](#_Toc5088415)

[2.4 Information 4](#_Toc5088416)

[2.5 Interfaces and dependencies 4](#_Toc5088417)

[2.6 Test and quality assurance 5](#_Toc5088418)

[3 Configuration 5](#_Toc5088419)

[3.1 System configuration 5](#_Toc5088420)

[3.2 Security configuration 5](#_Toc5088421)

[4 Operations 5](#_Toc5088422)

[4.1 Change management 5](#_Toc5088423)

[4.2 Access management 5](#_Toc5088424)

[4.3 Operational monitoring 5](#_Toc5088425)

[4.4 Functional updates 6](#_Toc5088426)

[4.5 Capacity management 6](#_Toc5088427)

[4.6 Backup and restore 6](#_Toc5088428)

[4.7 Decommissioning 6](#_Toc5088429)

[5 Troubleshooting 6](#_Toc5088430)

[6 Security 6](#_Toc5088431)

[6.1 Risk assessment 6](#_Toc5088432)

[6.2 Vulnerability assessment 6](#_Toc5088433)

[6.3 Security updates 6](#_Toc5088434)

[6.4 Security monitoring 6](#_Toc5088435)

[6.5 Incident handling 6](#_Toc5088436)

[7 Disaster recovery 6](#_Toc5088437)

[7.1 Disaster recovery 6](#_Toc5088438)

[7.2 Business continuity 6](#_Toc5088439)

[8 Service level agreements 7](#_Toc5088440)

[9 Regulatory compliance 7](#_Toc5088441)

[9.1 Sarbanes-Oxley Act (SOX) 7](#_Toc5088442)

# Introduction

## Purpose

This runbook provides the complete operational documentation of the **Data flow name data flow.**

The document should be used to understand how the system is configured and functions, including how to perform system administrative tasks. The primary audience for this document are personnel responsible for managing and operating the system.

## Scope

|  |  |
| --- | --- |
| **Functionality** | The **Data flow name data flow** transfers…<brief summary of functionality including data transfer type and frequency.> |
| **Components** | The main components of the **Data flow name data flow** are:   * <list the main components> |
| **Design notes** | Any notes about the data flow design. |

## Authoring rules

To assist in filling out the runbook correctly, the following applies:

* Highlighted, italicized text throughout the template is provided as background information to assist in creating the document. In the final version of the document, this text must be removed and/or replaced by system-specific information.
* Existing chapters or subchapters shall not be deleted. If a subchapter is considered irrelevant for the system, this must be specified in the body text of the subchapter.
* New subchapters can be added as required. When doing so, the table of contents must be updated.
* Linking to SOPs and information stored in other systems is encouraged.
* No confidential information shall be entered in the runbook itself (although referenced SOPs, with appropriate access control, can contain this type of information).

If the operational documentation is stored in another format than this word document (such as a dedicated system for managing system documentation), the bulleted list above still applies.

## Legal

This document contains information that is proprietary to Equinor ASA. Neither the document nor the information contained therein should be disclosed or reproduced in whole or in part, without express written consent of Equinor ASA.

The document and the information it contains shall be handled according to Equinor’s information classification scheme.

# Architecture

## Architecture overview

The main components in the system architecture are described in the table below. All components are OMNIA resources, with the exception of the <summary of the exception(s)>:

| *Component type* | *Feature(s)* | *System component name* | *Usage* |
| --- | --- | --- | --- |
| **Name** | Name | Name | Brief description |
| Name | Name | Brief description |
| Name | Brief description |
| … | … |
| Name | Brief description |
| Name |  | Brief description |
| **…** | … |  | … |
| **Name** | Name |  | Brief description |

## Hardware

This data flow uses shared hardware components only. See [section 2.5](#_Interfaces_and_dependencies_1) for an overview of shared components used.

## Software

| *Component type* | *Component name* | *OMNIA subscription* | *OMNIA resource group* | *Usage* | *Criticality* |
| --- | --- | --- | --- | --- | --- |
| **Name** | Name 1 | Name | Name | Dev | Medium |
| … | … | … | Test | Low |
| Name n | Name | Name | Prod | High |
| **…** | Name 1 | Name | Name | Dev | Medium |
| … | … | … | Test | Low |
| Name n | Name | Name | Prod | High |
| **Name** | Name 1 | Name | Name | Dev | Medium |
| … | … | … | Test | Low |
| Name n | Name | Name | Prod | High |

See [section 2.5](#_Interfaces_and_dependencies_1) for an overview of shared software components used.

## Information

| *Source data <feature providing data>* | *Description* |
| --- | --- |
| **Name** | Brief description |
| **…** | … |
| **Name** | Brief description |
|  |  |
| **Information security classification** | Open/Internal/Restricted/Confidential |
| **Legal risk assessment (LRA) status** |  |

The activities and data flow in the Azure Data factory (V2) pipeline is illustrated below. The diagram is copied from [DataFactory Explorer](https://common-datafactory-explorer.azurewebsites.net/dfv2/odet2rgdev/ODET2DFDev/) (open in Google Chrome).

<paste diagram here>

## Interfaces and dependencies

The data flow is dependent on the following components (all OMNIA resources, except the <exception(s>):

| *Component type* | *Component name* | *OMNIA resource group* | *Usage* | *Criticality* |
| --- | --- | --- | --- | --- |
| **Name** | Name | Name | Dev | Medium |
| Name | Name | Test | Low |
| Name | Name | Prod | High |
| **…** | Name | Name | Dev | Medium |
| Name | Name | Test | Low |
| Name | Name | Prod | High |
| **Name** | Name | Name | Dev | Medium |
| Name | Name | Test | Low |
| Name | Name | Prod | High |

## Test and quality assurance

The test environment (see component descriptions in sections [2.3](#_Software) and [2.5](#_Interfaces_and_dependencies)) is used for testing and quality assurance of the data flow. It is not used for testing data quality (integrity) after transfer. This is done in the development and production environments. The [Data flow delivery checklist](https://statoilsrm.sharepoint.com/:w:/r/sites/DataPlatformTeamTwo/Shared%20Documents/Checklists%20and%20templates/Data%20flow%20delivery%20checklist%20(template).docx?d=w021ffaf04f574eacab4538c1c2bfe2c3&csf=1&e=duIdKl) is used for quality assurance and control.

# Configuration

## System configuration

|  |  |
| --- | --- |
| **Configuration, custom code and deployment scripts** | Essential configuration data are included on the [first page in this document](#_top).The files containing the detailed definition and configuration of the Azure components described in [section 2.1](#_Architecture_overview) are all stored in the Equinor GitHub repository **DataLakers** (github.com/equinor/DataLakers), in the **projects** folder. This also includes deployment scripts and instructions. [If relevant:] App properties/settings are provided in the table below. |

|  |  |  |
| --- | --- | --- |
| *App* | *Property/setting* | *Value/description* |
| **Name** | Name | Value/description |
| … | … |
| Name | Value/description |
| **…** | Name | Value/description |
| … | … |
| Name | Value/description |
| **Name** | Name | Value/description |
| … | … |
| Name | Value/description |

## Security configuration

|  |  |  |
| --- | --- | --- |
| *Component type* | *System component name(s)* | *Access permissions outside Data Lakers team* |
| **Name** | Name (or See [section 2.1](#_Architecture_overview)) | Description |
| **…** | Name (or See [section 2.1](#_Architecture_overview)) | Description |
| **Name** | Name (or See [section 2.1](#_Architecture_overview)) | Description |

|  |  |
| --- | --- |
| **Source data extraction user password management** | Description |

# Operations

## Change management

Change management is incorporated in Data Lakers’ daily task management. The [Data flow delivery checklist](https://statoilsrm.sharepoint.com/:w:/r/sites/DataPlatformTeamTwo/Shared%20Documents/Checklists%20and%20templates/Data%20flow%20delivery%20checklist%20(template).docx?d=w021ffaf04f574eacab4538c1c2bfe2c3&csf=1&e=duIdKl) is used for quality assurance and control. The checklists documents who has been involved as developers and reviewers.

The change/release history is updated in the table below.

|  |  |  |  |
| --- | --- | --- | --- |
| *R* | *Released* | *Additions/changes compared to previous version* | *Developer(s)* |
| **x.y** | DD.MM.YYYY | Description | Shortname(s) |
| **…** | … | … | … |
| **1.0** | DD.MM.YYYY | Description | Shortname(s) |

## Access management

Access permissions for all Azure components except the SQL databases are managed using groups in Azure Active Directory, through the Azure portal. SQL database users and permissions are defined using SSMS.

All members of Data Lakers have administrator access to all system components in the development and test environments. Selected members have administrator access in the production environment. Access permissions outside Data Lakers are specified in [section 3.2](#_Security_configuration).

## Operational monitoring

Azure Log Analytics and the common OMNIA transfer log API are used for monitoring the data flow.

## Functional updates

The standard operating procedure (SOP) (link to be included) should be followed for deployment of functional updates in the system. Version specific deployment instructions are available in the DataLakers GitHub repository as described in [section 3.1](#_System_configuration).

## Capacity management

Capacity configuration of the software component(s) specified in [section 2.3](#_Software) must be discussed and clarified with the OMNIA core team.

## Backup and restore

Refer to procedures for OMNIA (link to be included).

## Decommissioning

Refer to procedures for OMNIA (link to be included).

# Troubleshooting

No specific tools or procedures are established, neither for error reporting nor management of enquiries from users.

Or enter any procedures (actions) in the table below – for each specific issue (case):

|  |  |
| --- | --- |
| *Case* | *Actions* |
| **Title** | Description |
| **…** | … |
| **Title** | Description |

# Security

## Risk assessment

Security risk assessment (SRA) has been done for all software components used. See [overview in OMNIA wiki](https://dataplatformwiki.azurewebsites.net/develop/componentoverview).

## Vulnerability assessment

Refer to [Standard Operating Procedure (SOP) – Vulnerability Management](http://team-2.statoil.com/sites/ts-47273/_layouts/DocIdRedir.aspx?ID=be9d78d4-3704-47b4-9ee9-881b87b7feb9&HintUrl=Metodikk%2fVuln+mgmt+SOP.docx).

## Security updates

Refer to procedures for OMNIA (link to be included) and [KB0035618](https://equinor.service-now.com/selfservice?id=kb_article&sys_id=6a5048ba4f97e2c0bd03ce318110c7f9).

## Security monitoring

Refer to procedures for OMNIA (link to be included).

## Incident handling

Refer to [SF103 - Handle safety and security incident](http://aris.statoil.no/?objectguid=f9469e01-b2be-11e0-43e7-828060af7619).

# Disaster recovery

## Disaster recovery

Refer to procedures for OMNIA (link to be included).

## Business continuity

Refer to plan for OMNIA (link to be included).

# Service level agreements

No service level agreement (SLA) is established for this system. Refer to SLA for OMNIA (link to be included).

# Regulatory compliance

## Sarbanes-Oxley Act (SOX)

Not applicable.