Data Integration Template

# Introduction

This Data Integration Template must be completed by anyone requesting data from the Institutional Data Feed Service (IDFS). It provides a standardised structure through which data requests can be made and ensures that every data request is supported by comprehensive documentation.

## Summary of data request

|  |  |
| --- | --- |
| Application Name |  |
| Application Owner Name(s) |  |
| Application Owner Department |  |
| System Administrators |  |
| System Customers |  |
| IDFS Reviewer |  |
| Date of Last Review |  |
| Notes |  |

## 1: Describe the application

### 1.1 Existing application

**Provide a brief summary of the application’s function.**

|  |
| --- |
|  |

**Provide a brief summary of existing data feeds to and from this application (if any exist).**

|  |
| --- |
|  |

### 1.2 IDFS requirements

**Describe the business benefit enabled by the data feed**

|  |
| --- |
|  |

**Provide a brief summary of the data requirements**

|  |
| --- |
|  |

**List any data for which Application is the authoritative source**

|  |
| --- |
|  |

## 2: Data required

**List the data that this application requires to perform its function**

|  |
| --- |
| **Input Data Requirements** |
| **Data name** | **Field type** | **Size** | **Nullable** | **Rules for data processing.** |
|  |  |  |  |  |
| ***Notes:***  |

## 3: Data integration method

Choose from one of the following techniques:

### Option (A) Secure File Transfer

Please DO NOT provide password/key data in this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Host | Local directory | Username | File name | Authentication methodPassword/private key |
|  |  |  |  |  |

|  |  |
| --- | --- |
| **File name** | Field delimiter |
| **Field Name** | **Size** | **Nullable** | **Description and comments** |
|  |  |  |  |
| **Notes:** |

### Option (B) Database update

Please DO NOT provide password/key data in this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type of database | Host | Login id | Database name | Authentication methodPassword/private key |
|  |  |  |  |  |

|  |  |
| --- | --- |
| **Table name** |  |
| **Column Name** | **Data type** | **Size** | **Nullable** | **Key** | **Description and comments** |
|  |  |  |  |  |  |
| **Notes:** |

### Option (C) Other e.g. Messaging system, Web service, XML

This may require a longer development time.

|  |
| --- |
|  |

## 4: Timing, frequency and critical periods

Please provide details of any specific timing and frequency requirements for your data feed. For example, the data feed to run nightly before a certain time to allow for downstream processing at a fixed time.

|  |
| --- |
|  |

Are there any times of year when the accuracy and timeliness of the data are especially critical? For example, during registration.

|  |
| --- |
|  |

## 5: Service owner responsibilities.

## Data protection responsibilities

Compliance with Data Protection policies and practices is the responsibility of the application owner. It is assumed that data is provided to systems whose owners are suitably aware of their data protection responsibilities. Advice on data protection is available from security colleagues in the IT Service, via a request to the IT service desk (it.servicedesk@ncl.ac.uk).

## Security Responsibilities

Similar to data protection responsibilities, it’s assumed that data is provided to systems whose owners are suitably aware of security best practices and their responsibilities to suitably secure their systems and keep them up to date. Advice on security is available from security colleagues in the IT Service, via a request to the IT service desk (it.servicedesk@ncl.ac.uk). Compliance with security policy may mean ensuring suppliers and or partners meet suitable security standards; ensuring that suppliers and partners are aware of and acting on their responsibilities is the application owners’ responsibility.

## Data retention policy compliance

All applications should have a data retention policy on the retention of records. Records should not be retained indefinitely and data purging procedures should be in place. It’s assumed that data is provided to systems whose owners are suitably aware of their data retention policies and procedures. Again, advice about these responsibilities can be sought from Information Security experts in the IT Service via a request to the IT service desk (it.servicedesk@ncl.ac.uk).

Are you satisfied that you are in a position to fulfil the responsibilities outlined above?

|  |
| --- |
|  |

## 6: Formalities

Request details filled in by

|  |
| --- |
|  |

Date request sent to IDFS:

|  |
| --- |
|  |