Integrated
Research Campus

UNIVERSITY OF LEEDS

Policy on Data Transfer

Version 1.0

Version Date 20/10/2016

Document Information

Reference	IRC DT P
Category	ISMS Documents
Title	IRC Policy on Data Transfer
Purpose	Policy that applies to data transfer to, from and within the IRC
Version	1.0
Status	Approved, Internal
Owner	IRC Information Governance Management Group
Author	Samantha Crossfield
Compliance	ISO 27001 for scope defined in IRC Framework of the Information Security Management System
Review plan	Set in the IRC IS Documentation Procedure
Related Documents	University of Leeds Information Protection Policy IRC Framework of the Information Security Management System

Version History

Version	Date	Change description
0.1	27/06/2016	Initial version
1.0	20/10/2016	Submitted for sign off

Sign-Off

Name	Date	Role
Barry Haynes		Chair of IGMG and Head of Enterprise Architecture, University of Leeds

Master version:

Signature…….

Table of Contents

1. Purpose

The Integrated Research Campus (IRC) is a University of Leeds Central IT provision. It provides secure technical infrastructure and services for research data handling, analytics, application processing and development. This document is part of the IRC information security management system (ISMS).

The IRC Framework of the Information Security Management System sets the IRC IS objectives and which of these are met through the procedures defined in this document.

This document sets the procedure for the **Transfer of Data** in and out of the IRC, and between secure zones in the IRC. This includes transfer between the IRC gateway, storage, data services and Virtual Research Environment (VRE) zones, and between firewalled applications and virtual machines within these zones (Figure 1). It sets out the ISMS scope boundary and how to manage data as it crosses this during transfer in and out of the IRC.

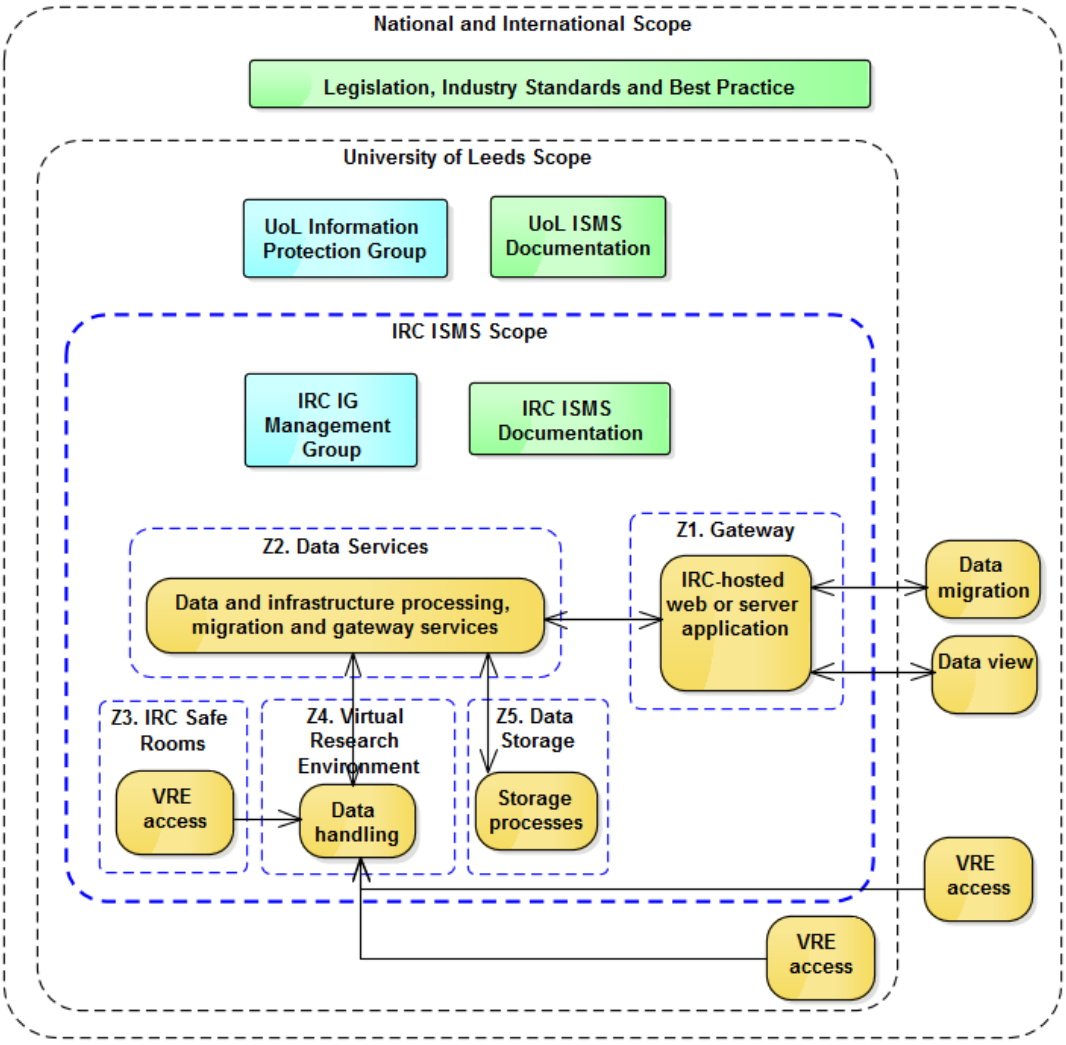

Figure 1: Representation of the IRC services (yellow) in the context of the five IRC zones (Z1-Z5) and the scopes of information security requirements.

2. Applicability

This document applies to all IRC users and IT staff involved in the transfer of data in, out, and within the IRC. The IRC Data Services Team ensures that data transfer happens in accordance with this document.

In line with the UK Information Commissioner, transfer is the conveyance "from one place, person, ownership, object, group, etc., to another".

Remote access of IRC-held data, even from abroad, is exempt. The IRC Information Governance (IG) Management Group oversees and maintains these procedures.

3. Transfer Principles

The following principles apply to all data transfer in, out and within the IRC scope:

1. Formal arrangement and agreements that surround the data sharing **must be** set up prior to data transfer
2. Agreements for datasets should, where it is not covered by other arrangements, define 'data type', 'fair processing', 'data usage – what for and how', 'data accuracy', 'handling duration', and the 'remit for transfer'
3. Data transfer **must be** in accordance with any ethical, legal, or governance requirements held upon the data, and justifiable in this context. The IRC Data Services Team will make all reasonable attempts to ascertain and log these requirements prior to transfer
4. Transfer of personal data **must be** undertaken in line with data protection legislation and the University of Leeds Code of Practice on Data Protection.
5. Personal data **must not** be transferred outside the European Economic Area without consent or legal justification. Such transfers must abide by the eighth principle of the Data Protection Act 1998
6. Transfer volume and frequency **must be** in accordance with the minimum required
7. Transfer arrangements **must** minimise any risk associated with the loss or improper use of the data being transferred
8. It is the 'IRC norm' to perform handling under a **Data Sharing Agreement** or **Open-Use Licence**
9. Manual or automated steps must be in place to check that transfers are in accordance with these principles

4. Preparation for Transfer

Data undergo manual and/or automated processing and review prior to transfer.

4.1. Data Processing

Data processing may be required prior to transfer:

1. All received data are virus-scanned within the IRC gateway zone
2. Data are checked manually or automatically for disclosure upon entry and prior to internal transfer or exit
3. Transfer review (Section 4.2) is based on data handling agreements and other legal and ethical requirements

4.2. Transfer Review

The transfer protocol and data are reviewed by the IRC Data Services Team through manual or automated processes prior to transfer.

Prior to transferring personal data, the Team review the consent or other ethico-legal framework to ensure it covers the proposed transfer. Alternatively, data may be de-identified or obfuscated at source. Where the data is held on the IRC infrastructure, this may be conducted by the IRC Data Services Team (with the appropriate ethical and governance approval).

IRC users may develop derived datasets from personal data held on IRC infrastructure.

1. The user prepares the derived dataset (they may request support from the IRC Data Services Team)
2. The user submits a data transfer request to the Data Services Team and places the derived data in a specified file
3. The Data Services Team review the derived extract using the ICO Anonymisation Code of Practice and apply UKDS-accredited statistical disclosure controls to ensure it is de-identified and classed as IRC Public
4. The Data Services Team release the dataset via the gateway zone

5. Transfer Procedures

While transfer procedures vary according to need, each procedure is arranged in accordance with the transfer principles (Section 3). The following steps apply to each transfer procedure:

- Each transferral utilises means, such as a file drop-off server, networked server, web application, transferrable media or attachments, which are appropriate to maintaining data confidentiality, integrity and availability.
- For each project and user, all allocated IRC servers, applications, VMs and services are firewalled – transfers across firewalls are monitored:
    - The IRC Data Services Team sets up firewalls to enable authorised transfer
    - Unauthorised attempts trigger an alert with the Data Services Team
- Password protection is applied to all files leaving the IRC with data that is not classified as IRC Public
- A two-stage authentication procedure is adopted whenever files are password protected prior to transfer

- The IRC Data Services Team makes all reasonable effort to verify the recipient when data is transferred from the IRC. Where there is doubt, transfer is postponed or cancelled
- Beyond the security requirements of the data, any further security mechanisms that can reasonably be employed during transfer must be utilised

5.1. Transfer Log

The IRC Data Services Team maintains a log of all transfers and transfer attempts:

1. Authorised transfers **are recorded** with a reference to a copy of any transfer agreements.
2. Incidents of risk from unauthorised attempts **are reported** to the IRC IG Management Group

The IRC transfer log records the following:

1. Unique asset ID, name and owner
2. IRC data classification *(as per the IRC Data Classification Procedure)*
3. Timeframe of data coverage
4. Data location/s within the IRC infrastructure
5. Transfer request ID, date and link to copy of the request
6. Request outcome with link to documentation
7. Data sharing approval type and link to documentation in asset folder
8. Data source (supplier and database / system)
9. Date of review / licence renewal submission and review requirements
10. Transfer method
11. Data raw file name and date received
12. Required destruction date and date of destruction
13. Data users in the IRC environment
14. Data recipient details

6. ISMS Scope

This section defines the boundary of the ISMS scope as it applies to the transfer of data in and out of the IRC.

6.1. Data Entry

Data transfer from external sources to IRC infrastructure involves data handling across the ISMS scope boundary (**Figure 1**). **Figure 2** shows the extent of the ISMS scope during data flow from such sources to, in this illustration, the IRC VRE.

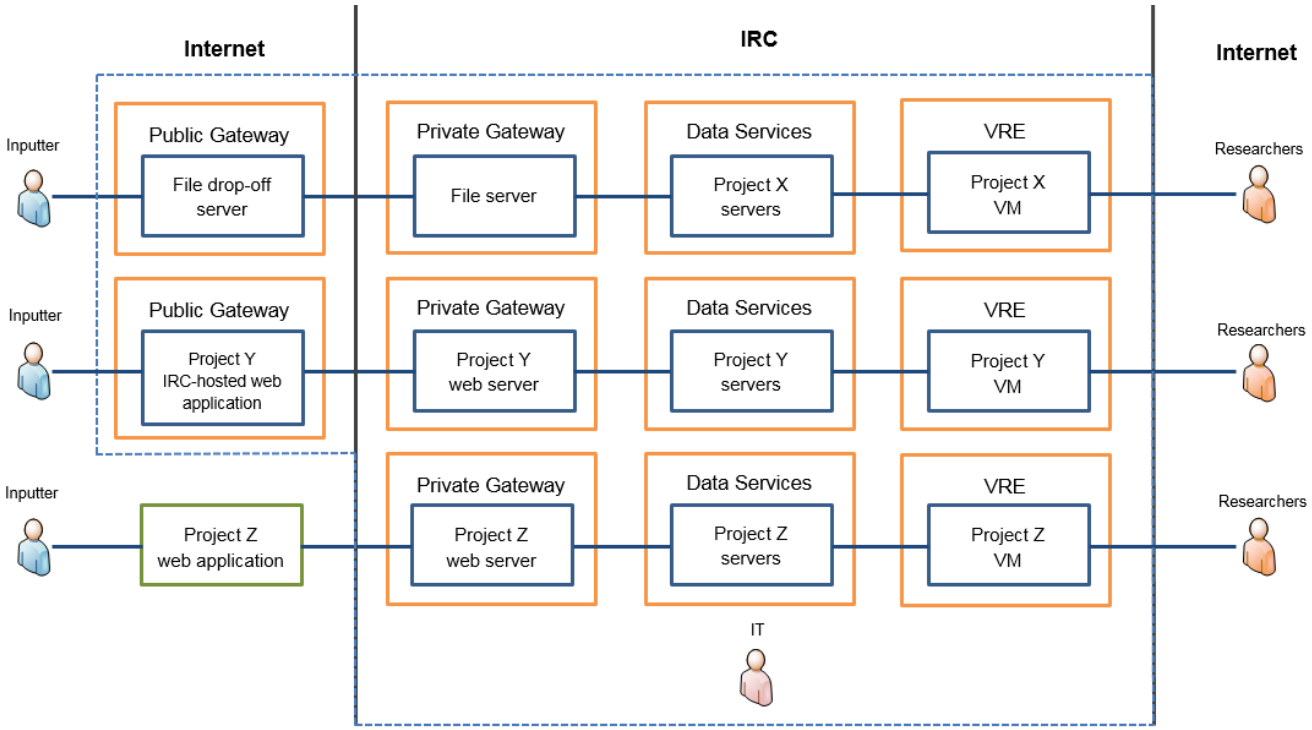

Figure 2 Flow from data source to the VRE for three example projects (X, Y, Z) using:

1. An IRC data drop-off server (X)
2. IRC-hosted web application (Y)
3. Non-IRC hosted web application (Z)

Orange lines represent firewalls, the blue dashed line is ISMS scope – anything beyond this falls in-scope upon crossing the dashed line.

6.2. Data Migration to External Facilities

There may be interplay between IRC and external infrastructure during the handling of data that has been defined as IRC Protect, IRC Confidential or IRC Secure. There are two routes:

1. The IRC Data Services can ‘take over’ the configuration of the facilities so that disclosive project data remains within the secure IRC environment.
   During this time the configuration of the facilities is within the ISMS scope.

2. Where the project has or produces data that is classified as IRC Unclassified (non-disclosive), or has an ethico-legal framework for the transfer, then this can be downloaded from the IRC to the external facilities.
   The data is then beyond scope upon leaving the IRC infrastructure.

As an example, **Figure 3** illustrates these two routes during with interplay between IRC and facilities at the Leeds Institute for Data Analytics (LIDA).

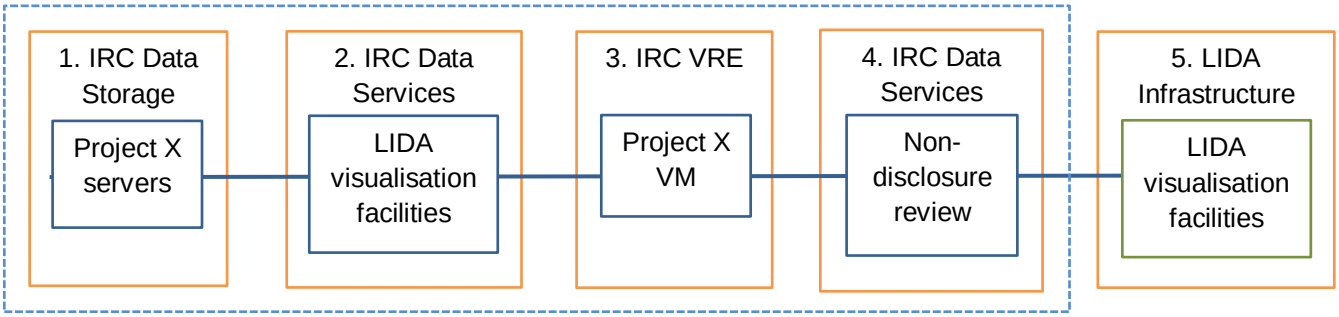

Figure 3 Example of LIDA visualisation facilities being used to analyse disclosive and non-disclosive data.

Orange lines represent firewalls and the blue dashed line is the ISMS scope.

The following steps correspond to the numbers in **Figure 3**:

1. Project data is stored on the **IRC** servers
2. **IRC** Data Services 'take over' the LIDA visualisation facilities (blocking access to local networks) so that disclosive data can be analysed on these facilities within the secure IRC environment
3. Post-visualisation data-sets are sent back to the **IRC** servers in between analysis sessions or to the IRC VRE for further analysis
4. The project submit a dataset for non-disclosure review and release into the **IRC** gateway zone in encrypted format
5. The user downloads the non-disclosive dataset for further analysis and dissemination using the **LIDA** visualisation facilities